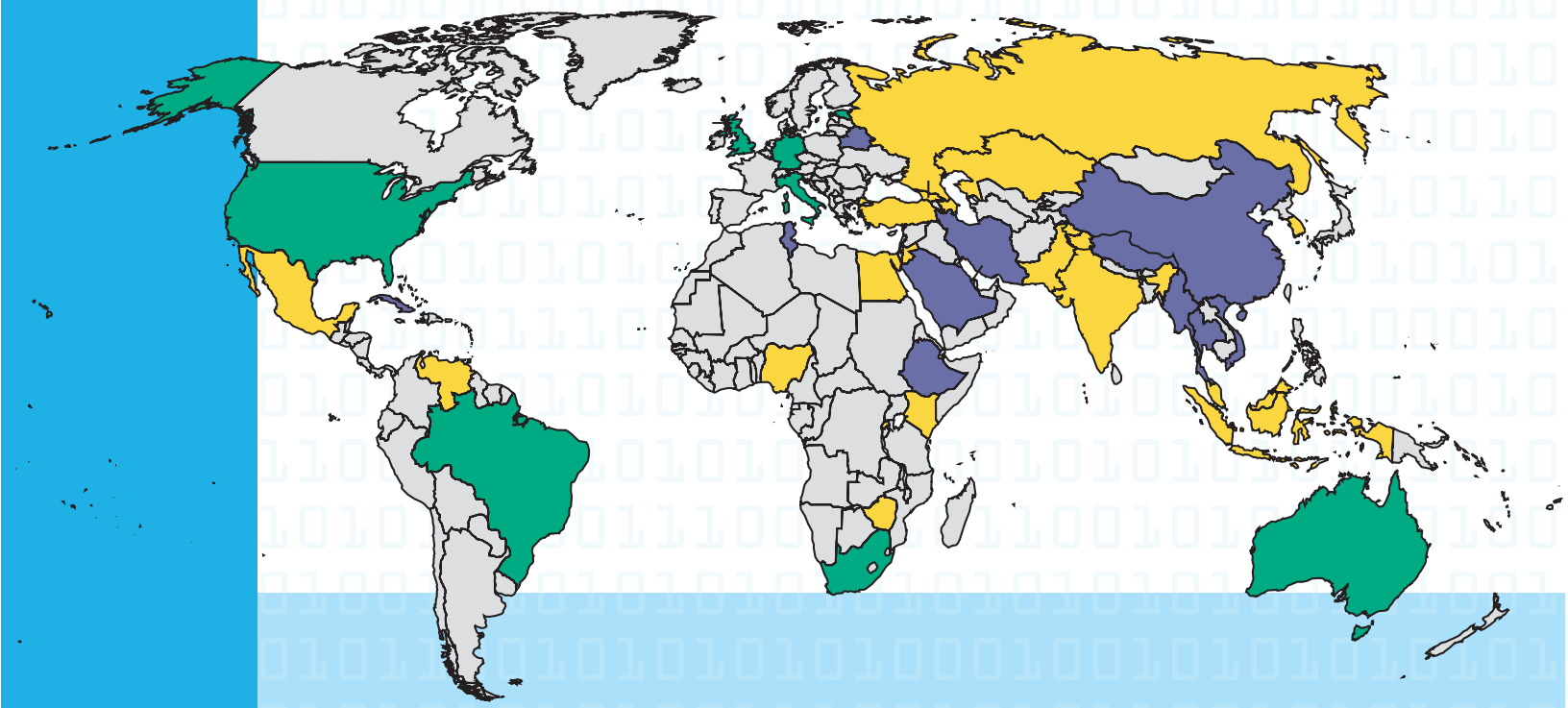
FREEDOM HOUSE

FREEDOM ON THE NET 2011

A GLOBAL ASSESSMENT OF INTERNET AND DIGITAL MEDIA



UNDEF The United Nations Democracy Fund

FREEDOM ON THE NET 2011

A Global Assessment of Internet and Digital Media

Sanja Kelly

Sarah Cook

EDITORS

EMBARGOED COPY

April 18, 2011

TABLE OF CONTENTS

ACKNOWLEDGMENTS

Completion of the *Freedom on the Net* publication would not have been possible without the tireless efforts of the following people.

As managing editor, Sanja Kelly directed the research, editorial, and administrative operations for the project, supported by Asia research analyst and assistant editor Sarah Cook. Together, they provided essential research and analysis, edited the country reports, and conducted field visits in Turkey, Malaysia, and South Africa. Over 40 external consultants served as report authors and advisors, and made an outstanding contribution by producing informed analyses of a highly diverse group of countries and complex set of issues. Tyler Roylance copyedited the volume and provided critical editorial and analytical insight throughout. Interns Abha Parekh and Sabrina Baum provided indispensable research, editorial, and administrative assistance.

General oversight was provided by Christopher Walker, director of studies. Helpful contributions and insights were made by Daniel Calingaert, deputy director of programs, Robert Guerra, internet freedom project director, as well as other Freedom House staff in the United States and abroad including Jake Dizard, Karin Karlekar, Rashweat Mukundu, Matthew Brady, Viviana Giacaman, Sherif Mansour, Miwa Kubosaki, Piet Khaidir, Julie Middleton, and Kerryn Shewitz. Experts from the Center for Democracy and Technology—Leslie Harris, Jim Dempsey, and Cynthia Wong—also provided valuable feedback.

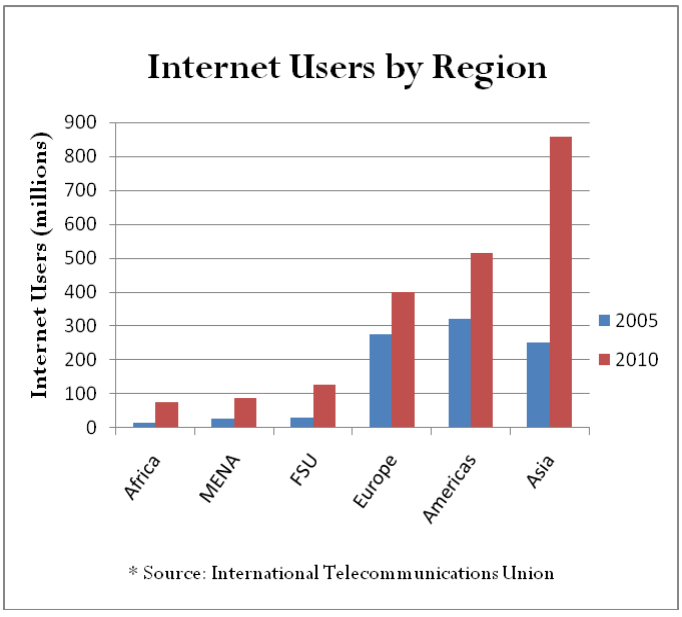
This publication was produced with the generous assistance of the United Nations Democracy Fund (UNDEF) and Google. Additional contributions were also made by the Dutch Ministry of Foreign Affairs and the United States Agency for International Development (USAID). The content of the publication is the sole responsibility of Freedom House and does not necessarily reflect the views of the United Nations, UNDEF or its Advisory Board, Google, the Dutch Ministry, USAID, or any other funder.

NEW TECHNOLOGIES, INNOVATIVE REPRESSION: Growing Threats to Internet Freedom

By Sanja Kelly and Sarah Cook

Over the past decade, and particularly in the last few years, the influence of the internet as a means to spread information and challenge government-imposed media controls has steadily expanded. This mounting influence directly corresponds to the growth in the number of users around the world: over two billion people now have access to the internet, and the figure has more than doubled in the past five years. However, as more people use the internet to communicate, obtain information, socialize, and conduct commerce, governments have stepped up efforts to regulate, and in some instances tightly control, the new medium. Reports of website blocking and filtering, content manipulation, attacks on and imprisonment of bloggers, and cyberattacks have all increased sharply in recent years.

To illuminate the nature of the emerging threats and identify areas of growing opportunity, Freedom House has conducted a comprehensive study of internet freedom in 37 countries around the globe. An earlier, pilot version was published in 2009, covering a sample of 15 countries. The new edition, *Freedom on the Net 2011*, assesses a wider range of political systems, while tracking improvements and declines in the countries examined two years ago. Over 40 researchers, most of whom are based in the countries they examined, contributed to the project by researching laws and practices relevant to the internet, testing accessibility of select websites, and interviewing a wide range of sources. Although the study's findings indicate that the threats to internet freedom are growing and have become more diverse, they also highlight a pushback by citizens and activists who have found ways to sidestep some of the restrictions and use the power of new internet-based platforms to promote democracy and human rights.



When the internet first became commercially available in the 1990s, very few restrictions on online communications and content were in place. Recognizing the economic potential of the new medium, many governments started investing heavily in telecommunications infrastructure, and internet-service providers (ISPs) sought to attract subscribers by creating online chat rooms and building communities of users around various topics of interest. Even the authorities in China, which today has the most sophisticated regime of internet controls, exerted very little oversight in the early days. However, as various dissident groups in the late 1990s began using the

internet to share information with audiences inside and outside the country, the government devoted tremendous human and material resources to the construction of a multilayered surveillance and censorship apparatus. Although China represents one of the most severe cases, similar dynamics are now becoming evident in many other countries.

Indeed, the country reports and numerical scores in this study reveal that a growing number of governments are moving to regulate or restrict the free flow of information on the internet. In authoritarian states, such efforts are partly rooted in the existing legal frameworks, which already limit the freedom of the traditional media. These states are increasingly blocking and filtering websites associated with the political opposition, coercing website owners into taking down politically and socially controversial content, and arresting bloggers and ordinary users for posting information that is contrary to the government's views. Even in more democratic countries—such as Brazil, India, Indonesia, South Korea, Turkey, and the United Kingdom—internet freedom is increasingly undermined by legal harassment, opaque censorship procedures, or expanding surveillance. The spread and intensification of internet controls in each country that showed decline generally conformed to one of the following three patterns:

Initial signs of politically motivated internet controls: In several countries that were previously free from most internet controls, the first signs of politicized censorship and user rights violations emerged, often in the period before or during elections. Many of these incidents represented the first time that a website in the country had been blocked, a user detained, or a restrictive law passed. This dynamic was particularly evident in Venezuela, Azerbaijan, Jordan, and Rwanda. In Venezuela, for example, users subscribing to internet services through the state-owned telecommunications firm CANTV reported that they were unable to access opposition-oriented blogs and a popular news site in the days surrounding parliamentary elections in September 2010. In Azerbaijan in 2009, the authorities temporarily blocked several websites that lampooned the president, and jailed two youth activists who posted a video that mocked the government.

Acceleration and institutionalization of internet controls: In countries where the authorities had already shown some tendency toward politically motivated controls over the internet, the negative trend accelerated dramatically, and new institutions were created specifically to carry out censorship. In Pakistan, for example, where temporary blocks have been common in recent years, a new Inter-Ministerial Committee for the Evaluation of Websites was established in mid-2010 to flag sites for blocking based on vaguely defined offenses against the state or religion. In Thailand, the government has long blocked internet content and taken legal action against users, particularly those posting information that is critical of the monarchy. However, the number of detained offenders and blocked sites sharply increased over the last two years, particularly while top officials had the authority to extrajudicially order blockings under a state of emergency that lasted from April to December 2010.

Strengthening of existing internet-control apparatus: Even in countries with some of the most robust censorship and internet surveillance systems in the world, measures were taken to eliminate loopholes and further strengthen the apparatus. In China, blogs on political and social issues were shut down, the space for anonymous communication has dwindled, and the

government has stepped up efforts to counter circumvention tools. In Bahrain, Iran, Ethiopia, and Tunisia, intensified censorship or user arrests came in the context of popular protests or contentious elections. Following the June 2009 elections in Iran, the country's centralized filtering system evolved to the point of being able to block a website nationwide within a few hours, and over 50 bloggers have been detained. In Vietnam, in addition to blocking websites, restricting some social-networking tools, and instigating cyberattacks, the authorities displayed their muscle by sentencing four activists to a total of 33 years in prison for using the internet to report human rights violations and express prodemocracy views.

The new internet restrictions around the globe are partly a response to the explosion in the popularity of advanced applications like Facebook, YouTube, and Twitter, through which ordinary users can easily post their own content, share information, and connect with large audiences. While mostly serving as a form of entertainment, over the last two years these tools have also played a significant role in political and social activism. In Egypt and Tunisia, for example, democracy advocates have relied heavily on Facebook to mobilize supporters and organize mass rallies. Similarly, Bahraini activists have used Twitter and YouTube to inform the outside world about the government's violent response to their protests. Even in Cuba, one of the most closed societies in the world, several bloggers have been able to report on daily life and human rights violations.

Many governments have started specifically targeting these new applications in their censorship campaigns. In 12 of the 37 countries examined, the authorities consistently or temporarily imposed total bans on YouTube, Facebook, Twitter, or equivalent services. Moreover, the increased user participation facilitated by the new platforms has exposed ordinary people to some of the same punishments faced by well-known bloggers, online journalists, and human rights activists. Among other recent cases, a Chinese woman was sent to a labor camp over a satirical Twitter message, and an Indonesian housewife faced high fines for an e-mail she sent to friends complaining about a local hospital. Because new technologies typically attract the young, some of those arrested have been teenagers, including an 18-year old Iranian blogger writing about women's rights and a 19-year old Tibetan detained after looking at online photographs of the Dalai Lama.

In 23 of the 37 countries assessed, a blogger or other internet user was arrested for content posted online.

KEY FINDINGS

The 2011 edition of *Freedom on the Net* identifies a growing set of obstacles that pose a common threat to internet freedom in many of the countries examined. Of the 15 countries covered in the pilot, a total of 9 registered score declines over the past two years. The newly added countries lack earlier scores for comparison, but conditions in at least half of them suggest a negative trajectory, with increased government blocking, filtering, legal action, and intimidation to prevent users from accessing unfavorable content. In cases where these tactics are deemed ineffective or inappropriate, authorities have turned to cyberattacks, misinformation, and other indirect methods to alter the information landscape.

Political Content Increasingly Blocked, Transparency Lacking

Governments around the world have responded to soaring internet penetration rates and the rise of user-generated content by establishing mechanisms to block what they deem to be undesirable information. In many cases, the censorship targets content involving illegal gambling, child pornography, copyright infringement, or the incitement of hatred or violence. However, a large number of governments are also engaging in deliberate efforts to block access to information related to politics, social issues, and human rights.

Of the 37 countries examined, the governments of 15 were found to engage in substantial blocking of politically relevant content. In these countries, instances of websites being blocked are not sporadic or limited in scope. Rather, they are the result of an apparent national policy to restrict users' access to dozens, hundreds, or most often thousands of websites, including those of independent and opposition news outlets, international and local human rights groups, and individual blogs, online videos, or social-networking groups.

Countries with substantial censorship of political or social issues in 2009–10:

Bahrain, Belarus, Burma, China, Cuba, Ethiopia, Iran, Kazakhstan, Pakistan, Saudi Arabia, South Korea, Thailand, Tunisia, Turkey, Vietnam

Website blocking is typically implemented by ISPs acting on instructions from a government agent, judge, or other appointed entity, whose orders may apply to a particular domain name, an internet-protocol (IP) address, or a specific URL. ISPs keep track of and periodically receive updates on the resulting blacklists of banned sites. In a small number of countries, the filtering technology employed is more sophisticated, and can scan users' browsing requests for certain banned keywords. Keyword filtering is much more nuanced, enabling access to a given website but not to a particular article containing a sensitive keyword in its URL path. Among the countries studied, China, Iran, and Tunisia are known to have such systems in place. In China, which boasts the world's most comprehensive censorship apparatus, keyword filtering is evident in instant-messaging services as well, having been built into the software of popular messaging programs like TOM Skype and QQ.

Two of the countries categorized by Freedom House as electoral democracies—Turkey and South Korea—were also found to engage in substantial political censorship. In Turkey, a range of advanced web applications were blocked, including the video-sharing website YouTube, which was not accessible in Turkey from May 2008 to October 2010. South Korean authorities blocked access to an estimated 65 North Korea–related sites, including the official North Korean Twitter account, launched in August 2010. Meanwhile, the governments of Australia, Indonesia, and Italy introduced proposals that would enable automated filtering by ISPs, create a state-led multimedia content screening entity, and extend prescreening requirements from television broadcasting to video-hosting websites, respectively. By the end of 2010, these proposals had been set aside or amended to remove the most egregious requirements.

One aspect of censorship was evident across the full spectrum of countries studied: the arbitrariness and opacity surrounding decisions to restrict particular content. In most nondemocratic settings, there is little government effort to inform the public about which content is censored and why. In many cases, authorities avoid confirming that a website has been

deliberately blocked and instead remain silent or cite "technical problems." Saudi Arabia does inform users when they try to access a blocked site, and the rules governing internet usage are clearly articulated on government portals, but as in many countries, the Saudi authorities often disregard their own guidelines and block sites at will. Even in more transparent, democratic environments, censorship decisions are often made by private entities and without public discussion, and appeals processes may be onerous, little known, or nonexistent.

The widespread use of circumvention tools has eased the impact of content censorship and at times undermined it significantly. Such tools are particularly effective in countries with a high degree of computer literacy or relatively unsophisticated blocking techniques. For example, YouTube remained the eighth most popular website among Turkish users despite being officially blocked in that country for over two years, and the number of Vietnamese Facebook users doubled from one to two million within a year after November 2009, when the site became inaccessible by ordinary means. Users need special skills and knowledge to overcome blockages in countries such as China and Iran, where filtering methods are more sophisticated and the authorities devote considerable resources to limiting the effectiveness of circumvention tools. Still, activists with the requisite abilities managed to communicate with one another, discuss national events in an uncensored space, and transmit news and reports of human rights abuses abroad.

Cyberattacks Against Regime Critics Intensify

Some governments and their sympathizers are increasingly using technical attacks to disrupt activists' online networks, eavesdrop on their communications, and cripple their websites. Such attacks were reported in at least 12 of the countries covered in this study. However, attacks perpetrated by nonstate actors for ordinary criminal purposes are also a growing problem, particularly as internet penetration deepens and more users turn to the medium for shopping, banking, and other activities.

China has emerged as a major global source of cyberattacks. Although not all attacks originating in the country have been explicitly traced back to the government, their scale, organization, and chosen targets have led many experts to conclude that they are either sponsored or condoned by Chinese military and intelligence agencies. The assaults have included denial-of-service (DoS) attacks on domestic and overseas human rights groups, e-mail messages to foreign journalists that carry malicious software capable of spying on the recipient's computer, and large-scale hacking raids on the information systems of over 30 financial, defense, and technology companies, most of them based in the United States. In addition, independent analysts have detected cyberespionage networks that extend to 103 countries as part of an effort to spy on the Tibetan government-in-exile and its foreign government contacts.

As with offline forms of violence and intimidation, governments seem most likely to resort to cyberattacks when their power is threatened by disputed elections or some other political crisis. In Iran, for example, during the mass protests that followed the June 2009 presidential election, many opposition news sites were disabled by intense DoS attacks, and there is technical evidence confirming that government-owned IP addresses were used to launch the assaults. A group calling itself the Iranian Cyber Army, which operates under the command of the Islamic Revolutionary

Guard Corps, managed to hack a number of other sites with a mix of technical methods and forgery.

Similarly, in the wake of fraudulent elections in Belarus in December 2010, the government initiated DoS attacks against opposition websites, dramatically slowing down their connections and in some instances rendering them completely inaccessible. Belarusian authorities also engaged in a type of web forgery designed to confuse users and provide false information. For example, the country's largest ISP, the state-owned Belpak, redirected users from independent media sites to nearly identical clones that provided misleading information, such as the incorrect location of a planned opposition rally.

Countries where websites or blogs of government opponents faced cyber attacks in 2009-2010:

Bahrain, Belarus, Burma, China, Iran, Kazakhstan, Malaysia, Russia, Saudi Arabia, Thailand, Tunisia, Vietnam

The Tunisian regime of President Zine al-Abidine Ben Ali accelerated its hacking activity in the run-up to the January 2011 uprising that drove it from power. Security officials regularly broke into the e-mail, Facebook, and blogging accounts of opposition and human rights activists, either deleting specific material or simply collecting intelligence about their plans and contacts.

Governments Increasingly Exploit Centralized Infrastructure and Built-In Internet Chokepoints

Although it often goes largely unnoticed, centralized government control over a country's connection to international internet traffic poses a significant threat to online free expression and privacy, particularly at times of political turmoil. In about a third of the states examined, the authorities have exploited their control over infrastructure to limit widespread access to politically and socially controversial content, or in extreme cases, to cut off access to the internet entirely.

This centralization can take several forms. In Ethiopia and Cuba, for example, state-run telecommunications companies hold a monopoly on internet service, giving them unchecked control over users' ability to communicate with one another and the outside world. Elsewhere, the state-run company's control of the market is not complete, but its dominance is sufficient to significantly influence people's access to information. Thus when CANTV in Venezuela or Kazakhtelecom in Kazakhstan block a website, it becomes inaccessible to the vast majority of internet users.

As a growing number of governments liberalize the ISP market, such centralization may become less obvious. In countries including Egypt and Belarus, a state-controlled company owns the country's network of copper wires or fiber-optic cables and sells bandwidth downstream to a variety of retail-level ISPs. In China, Vietnam, and Saudi Arabia, an array of three to eight international gateways are available to multiple, economically competitive ISPs, yet ultimate control over the country's connectivity rests with the government.

Of the 37 countries assessed, 19 had at least a partially centralized and government-controlled international connection. Authorities in at least 12 of these were known to have used their leverage to restrict users' access to politically relevant information or engage in widespread

surveillance. Egypt joined the list in January 2011, when officials shut down the internet nationwide for five days in an unsuccessful attempt to curb antigovernment protests. Technicians reportedly cut off almost all international traffic flowing through a tiny number of portals, while ISPs, particularly state-owned Telecom Egypt, removed the routes to Egypt's networks from global routing tables—the mechanism that provides pathways for users' computers to connect to requested websites. The operation was accomplished within the span of one hour.

The Egyptian case demonstrates that at times of political unrest, authoritarian leaders do not hesitate to exploit infrastructural controls to protect their rule, even if it causes massive disruptions to economic activity and personal communications. Several other instances of this "kill switch" phenomenon have occurred in recent years. In 2007, at the height of a wave of popular protests led by Buddhist monks in Burma, state-run ISPs cut off the country's internet connection from September 27 to October 4. More recently, from July 2009 to May 2010, the Chinese authorities severed all connections to the northwestern region of Xinjiang while security forces carried out mass arrests in the wake of ethnic violence. Local government websites and other content hosted within Xinjiang remained accessible, but the region's 20 million residents were cut off from outside information and a range of services used daily by individuals and businesses—including e-mail, instant messaging, and blog-hosting.

Countries with at least partially centralized and government-controlled internet connections:

Azerbaijan, Bahrain, Belarus, Burma, China, Cuba, Egypt, Ethiopia, Iran, Jordan, Kazakhstan, Malaysia, Saudi Arabia, Thailand, Tunisia, Turkey, Venezuela, Vietnam, Zimbabwe

In addition to outright shutdowns, a centralized, state-controlled internet infrastructure facilitates two other types of restrictions: the deliberate slowing of connection speeds and the imposition of a nationwide system of filtering and surveillance. During opposition protests in Iran in the summer of 2009, authorities sharply reduced the speed of network traffic, making it difficult to conduct basic online activities like opening e-mail messages. Uploading a single image could take up to an hour. In early 2011, as protests began flaring up across the Middle East, the Bahraini government selectively slowed down internet connections at newspaper offices, hotels, and homes. The prime example of a centralized filtering system is China's so-called Great Firewall, but other countries, including Iran and Saudi Arabia, also use such systems to enforce nationwide censorship and monitor dissident activity.

Offline Coercion, Online Manipulation Alter Available Information

Rather than relying exclusively on technological sophistication to control internet content, many governments employ cruder but nevertheless effective tactics to delete and manipulate politically or socially relevant information. These methods are often ingenious in their simplicity, in that their effects are more difficult to track and counteract than ordinary blocking.

One common method is for a government official to contact a content producer or host, for example by telephone, and request that particular information be deleted from the internet. In some cases, individual bloggers or webmasters are threatened with various reprisals should they refuse the request. Increasingly, governments and their supporters are also taking advantage of

international hosting platforms' complaint mechanisms to have user-generated content removed. Over the past two years, activists from China, Egypt, Ethiopia, Mexico, and Tunisia found that their YouTube videos or Facebook accounts had been removed or disabled after complaints were filed, apparently by regime supporters. In several of these instances, the content was restored once the problem was brought to the hosting company's attention, but the threat of a blanket ban is sometimes enough to induce large websites to meet governments' specific deletion demands.

A certain set of countries have laws in place to hold content providers and hosts legally responsible for what others post on their sites. Such provisions effectively force the site owner to screen all user-generated content and delete what might be deemed offensive by the authorities. Long-standing laws in China have led internet companies there to employ hundreds of thousands of people responsible for monitoring and censoring online videos, bulletin-board discussions, blog posts, and microblog messages. Nevertheless, in 2009 and 2010, the Chinese authorities adopted various measures to increase pressure on private websites, obliging them to be more vigilant and prevent content from slipping through the cracks. In Thailand, Kazakhstan, Vietnam, and Venezuela, new laws or directives promulgated since 2007 have led to an increase in this type of censorship. In Thailand, for instance, online news outlets are legally responsible for comments posted by readers, and at least one editor is facing criminal charges over reader comments that were critical of the monarchy. In Vietnam and Venezuela, some webmasters and bloggers have disabled the comment feature on their sites to avoid potential liability.

In addition, a range of governments have deployed manpower and resources to proactively manipulate online discussion and bolster progovernment views. Thailand has military units assigned to countering online criticism of the monarchy, and Burma has established a blogging committee in each ministry. Elsewhere, those recruited and paid for such tasks may be ordinary citizens, often youth. Thus China has cadres, known as the "50 Cent Party" for their supposed per-comment fees, who are employed to post progovernment remarks on various online forums, and recruiting advertisements for similar commentators have reportedly begun to appear on Russian job sites. Government-sponsored posts aim not only to defend the leadership and its policies, but also to discredit opposition voices or human rights activists, and to deceive everyday users. During postelection protests in Iran, for example, government supporters posted fake user-generated content to Twitter and YouTube to mislead protesters and journalists.

In a somewhat different manipulation technique, search-engine providers in some countries, most notably China, are required to adjust search results to match government-imposed criteria, for instance by only offering government-affiliated sources on particular topics. In addition to displeasure over a series of cyberattacks, this obligation was at the center of Google's decision to withdraw from China in early 2010.

COUNTRIES AT RISK

After reviewing the findings for the 37 countries covered in this edition of *Freedom on the Net*, Freedom House has identified five that are at particular risk of suffering setbacks related to internet freedom in 2011 and 2012. A number of other countries showed deterioration over the past two years and may continue to decline, but the internet controls in these states—which include Bahrain, China, and Iran—are already well developed. By contrast, in most of the five countries listed below, the internet remains a relatively unconstrained space for free expression, even if there has been some obstruction of internet freedom to date. These countries also typically feature a repressive environment for traditional media, as well as an internet penetration rate of at least 25 percent, meaning the internet is both vitally important and in significant danger of repression.

Thailand

Internet users in Thailand have played a significant role in challenging the political establishment and the role of the monarchy in Thai politics since the military coup of 2006. This has provoked efforts by the government and military to control the free flow of information and commentary online. Although the government has been blocking some internet content since 2003, over the past two years online censorship has increased in both scale and scope, affecting tens of thousands of websites by the end of 2010, including independent news outlets and human rights groups. Restrictions intensified between April and December 2010, when a state of emergency allowed the authorities to extrajudicially block any website. Dozens of people have been charged under various laws for expressing their views online, particularly those that are critical of the monarchy. As of the end of 2010, many of these cases had yet to be decided. The country's political turmoil has continued, and parliamentary elections are tentatively scheduled for December 2011, raising the likelihood of additional backsliding on freedom of expression issues. In a worrying sign, a Thai judge in March 2011 sentenced a web developer to 13 years in prison for comments he posted and for refusing to remove the remarks of others.

Russia

Given the elimination of independent television channels and the tightening of press restrictions since 2000, the internet has become Russia's last relatively uncensored platform for public debate and the expression of political opinions. However, even as access conditions have improved, internet freedom has eroded. In the last two years, the country's first high-profile cases of technical blocking were reported, while tactics for proactively manipulating discussion in the online sphere were refined. Russian bloggers faced increasing intimidation: at least 25 cases of harassment of bloggers by the authorities occurred in 2009 and 2010, including 11 arrests. Greater efforts to increase government influence over the internet are anticipated as the country prepares for parliamentary elections in December 2011 and a presidential election in early 2012. In March 2011, bloggers reportedly uncovered evidence that Russian officials were hiring users to post

comments that would shape a "positive image" of the ruling United Russia party and "form a negative attitude" toward the author of a targeted blog.

Venezuela

While restrictions on broadcast media outlets have grown in recent years, the internet has remained relatively free, with blogs, Facebook, and Twitter becoming important spaces for the free diffusion of information. Opposition groups have used these platforms to mobilize support, and the authorities have responded with some attempts to restrict online content, though to date they have not engaged in large-scale filtering or blogger arrests. There have been periodic interruptions of access to opposition or independent websites, efforts to intimidate websites into censoring the comments of their users, and several prosecutions for information posted on Twitter. Perhaps the most worrying recent development is the passage in December 2010 of laws that increased state control over telecommunications networks and laid the foundation for website managers and service providers to be required to censor the comments of users. President Hugo Chávez had declared in March 2010 that the internet could not be "a free thing where you do and say whatever you want," and progovernment lawmakers were spurred to act in December following opposition gains in September parliamentary elections. The country is now preparing for a presidential election in 2012, and the state-run telecommunications firm CANTV has a record of apparently restricting access to websites and blogs at sensitive times, suggesting that there is a strong possibility of increased censorship and harassment of internet users in the coming months.

Zimbabwe

Internet access remains limited in Zimbabwe, but the number of mobile-phone users has increased rapidly since early 2009, from less than 10 percent of the population to nearly 50 percent by the end of 2010. While the regime of President Robert Mugabe has committed rampant human rights abuses and exercised strict control over the traditional media, the internet is nominally free from government interference. Nevertheless, there are indications that the government has a strong desire to control new information and communication technologies (ICTs), particularly mobile phones. The 2007 Interception of Communications Act allows the authorities to monitor telephone and internet traffic, and requires service providers to intercept communications on the state's behalf. In addition, some content restrictions and registration requirements related to mobile phones have been imposed in recent years. Parliamentary elections are likely to take place in late 2011, internet access via mobile phones is increasing, and there are a number of influential Zimbabwean news sites based in foreign countries, all of which may tempt Mugabe and his ZANU-PF party to increase ICT controls. Given the prevalence of mobile-phone use, this could take the form of censorship of text-messaging or even a "kill switch" action to disable the entire network.

Jordan

Jordan prides itself on offering broader freedom to use the internet than many other Middle Eastern countries. Nonetheless, internet users are aware that their browsing history, comments, and posted materials may be monitored by the authorities. Until recently, the government's interest in maintaining this direct access to public opinion seemed to have outweighed its impulses to control content. In August 2010, despite objections from civil society, the government adopted a new law on cybercrimes that could be used to limit free expression on the internet. For example, it prohibits the posting of any previously nonpublic information relevant to foreign affairs, national security, the national economy, or public safety. Many bloggers and web users have expressed concern that the government could exploit the ambiguous definitions for each of these categories and use the law selectively to silence its critics. Currently, outright blocking of websites by the authorities remains rare, but website owners often remove material after receiving informal complaints via telephone from government officials, and several popular news websites have been subjected to hacking attacks after posting sensitive material. In February 2011, Ammonnews.net was hacked and temporarily disabled after its editors refused to comply with security agents' demands to remove a statement in which Jordanian tribesmen called for democratic and economic reforms.

FREEDOM ON THE NET 2011: GLOBAL SCORES

Freedom on the Net aims to measure each country's level of internet and new media freedom. Each country receives a numerical score from 0 (the most free) to 100 (the least free), which serves as the basis for an internet freedom status designation of Free (0-30 points), Partly Free (31-60 points), or Not Free (61-100).

Ratings are determined through an examination of three broad categories: obstacles to access, limits on content, and violation of user rights.

- **Obstacles to Access:** assesses infrastructural and economic barriers to access; governmental efforts to block specific applications or technologies; and legal, regulatory and ownership control over internet and mobile phone access providers.
- **Limits on Content:** examines filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism.
- **Violations of User Rights:** measures legal protections and restrictions on online activity; surveillance; privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.

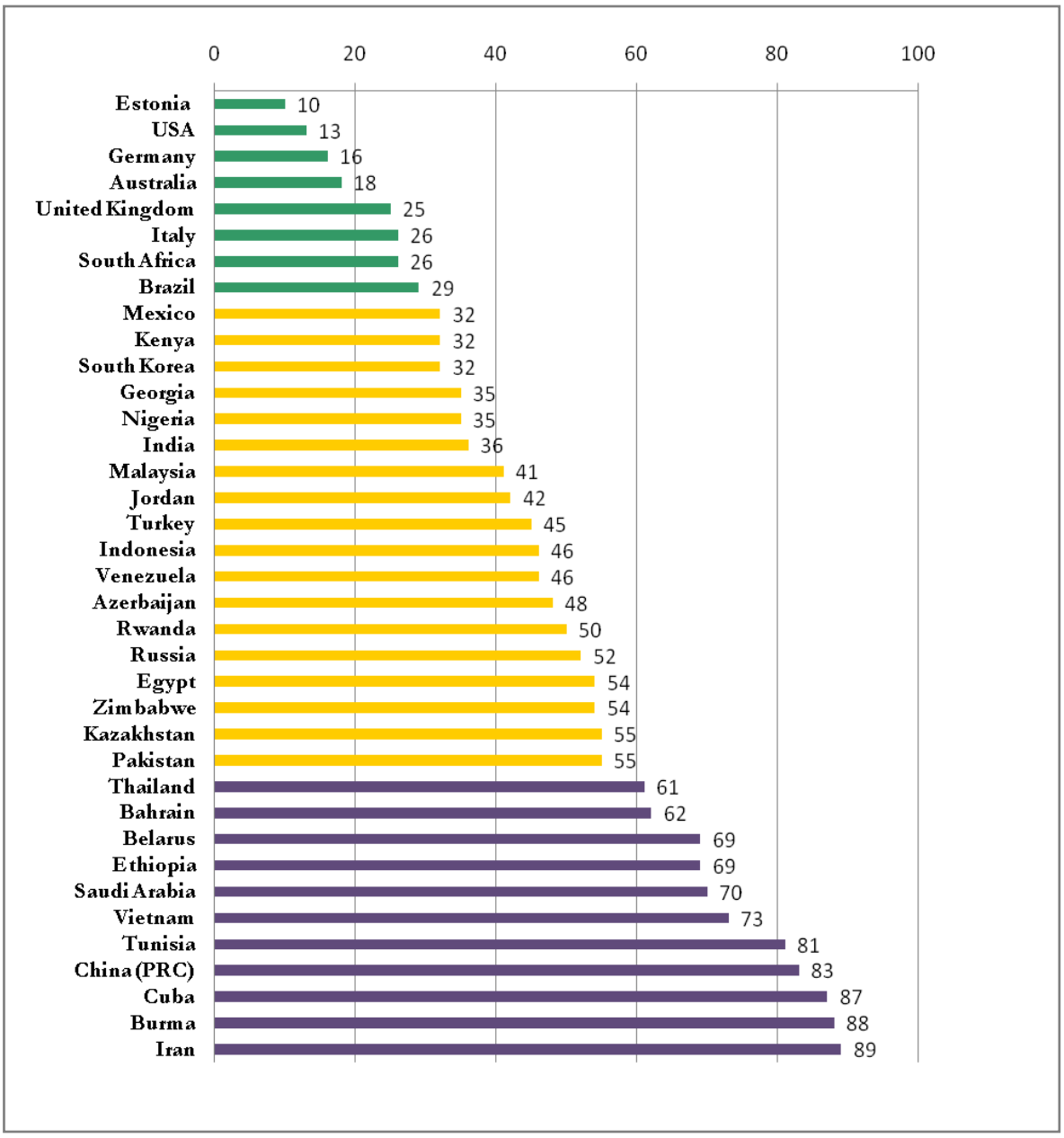
COUNTRY	*FREEDOM ON THE NET* STATUS	*FREEDOM ON THE NET* TOTAL *0-100 Points*	A SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
Estonia	**Free**	**10**	2	2	6
USA	**Free**	**13**	4	2	7
Germany	**Free**	**16**	4	5	7
Australia	**Free**	**18**	3	6	9
UK	**Free**	**25**	1	8	16
Italy	**Free**	**26**	6	8	12
South Africa	**Free**	**26**	7	9	10

COUNTRY	*FREEDOM ON THE NET* STATUS	*FREEDOM ON THE NET* TOTAL *0-100 Points*	A SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
Brazil	**Free**	**29**	7	7	15
Kenya	**Partly Free**	**32**	12	9	11
Mexico	**Partly Free**	**32**	12	10	10
South Korea	**Partly Free**	**32**	3	12	17
Georgia	**Partly Free**	**35**	12	10	13
Nigeria	**Partly Free**	**35**	13	10	12
India	**Partly Free**	**36**	12	8	16
Malaysia	**Partly Free**	**41**	9	11	21
Jordan	**Partly Free**	**42**	12	11	19
Turkey	**Partly Free**	**45**	12	16	17
Indonesia	**Partly Free**	**46**	14	13	19
Venezuela	**Partly Free**	**46**	15	13	18
Azerbaijan	**Partly Free**	**48**	15	15	18
Rwanda	**Partly Free**	**50**	14	19	17
Russia	**Partly Free**	**52**	12	17	23
Egypt	**Partly Free**	**54**	12	14	28
Zimbabwe	**Partly Free**	**54**	16	15	23
Kazakhstan	**Partly Free**	**55**	16	22	17
Pakistan	**Partly Free**	**55**	16	17	22

COUNTRY	*FREEDOM ON THE NET* STATUS	*FREEDOM ON THE NET* TOTAL *0-100 Points*	A SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
Thailand	**Not Free**	**61**	12	23	26
Bahrain	**Not Free**	**62**	11	22	29
Belarus	**Not Free**	**69**	19	23	27
Ethiopia	**Not Free**	**69**	21	26	22
Saudi Arabia	**Not Free**	**70**	14	27	29
Vietnam	**Not Free**	**73**	16	25	32
Tunisia	**Not Free**	**81**	21	28	32
China	**Not Free**	**83**	19	28	36
Cuba	**Not Free**	**87**	24	30	33
Burma	**Not Free**	**88**	23	29	36
Iran	**Not Free**	**89**	21	29	39

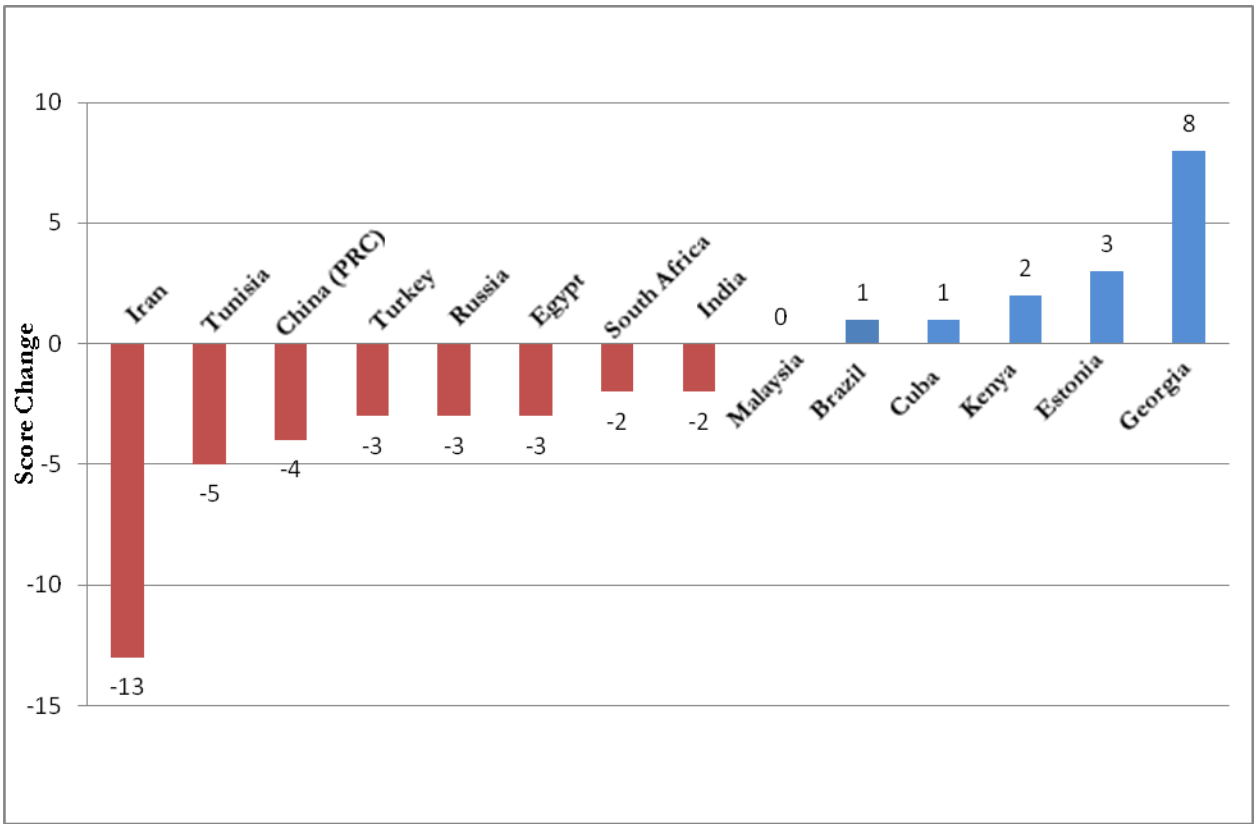
FREEDOM ON THE NET 2011: GLOBAL GRAPHS

37-COUNTRY SCORE COMPARISON (0 Best, 100 Worst)



* A green-colored bar represents a status of **"Free,"** a yellow-colored one, the status of **"Partly Free,"** and a purple-colored one, the status of **"Not Free"** on the *Freedom of the Net* Index.

SCORE CHANGES *FREEDOM ON THE NET 2009 VS. 2011*



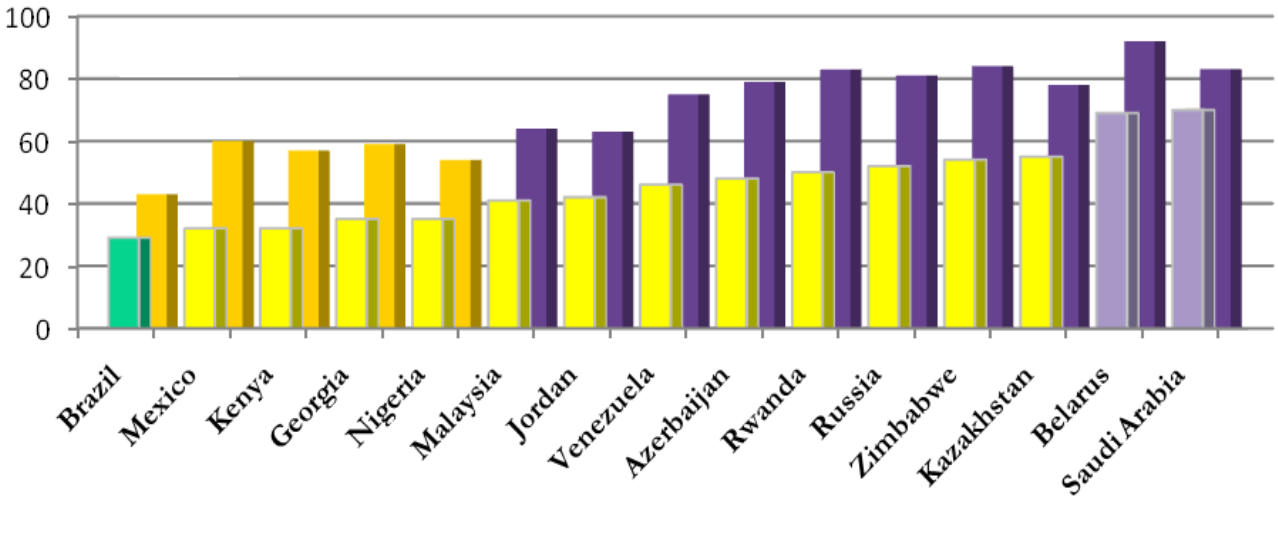
COUNTRY	FOTN 2009	FOTN 2011	TRAJECTORY
Brazil	30	29	↑
China	79	83	↓
Cuba	88	87	↑
Egypt	51	54	↓
Estonia	13	10	↑
Georgia	43	35	↑
India	34	36	↓
Iran	76	89	↓

COUNTRY	FOTN 2009	FOTN 2011	TRAJECTORY
Kenya	34	32	↑
Malaysia	41	41	**No change**
Russia	49	52	↓
South Africa	22	26	↓
Tunisia	76	81	↓
Turkey	42	45	↓
United Kingdom	23	25	↓

COUNTRIES AT RISK: INTERNET FREEDOM VS. PRESS FREEDOM

Among the 37 countries covered in this study, one notable contingent of states were those where the internet remains a relatively unobstructed domain of free expression when compared to a more repressive or dangerous environment for traditional media. This difference is evident from the comparison between a country's score on Freedom House's *Freedom on the Net 2011* assessment and its score on the *Freedom of the Press 2010* study.

The figure below is a graphical representation of this phenomenon, focusing on the 15 countries in this edition where the gap between their performance on the two surveys is 10 points or greater. This difference reflects the potential pressures in both the short and long term on the space for online expression. Among the 15 are several of the states identified as "countries at risk:" Jordan, Russia, Venezuela, and Zimbabwe.

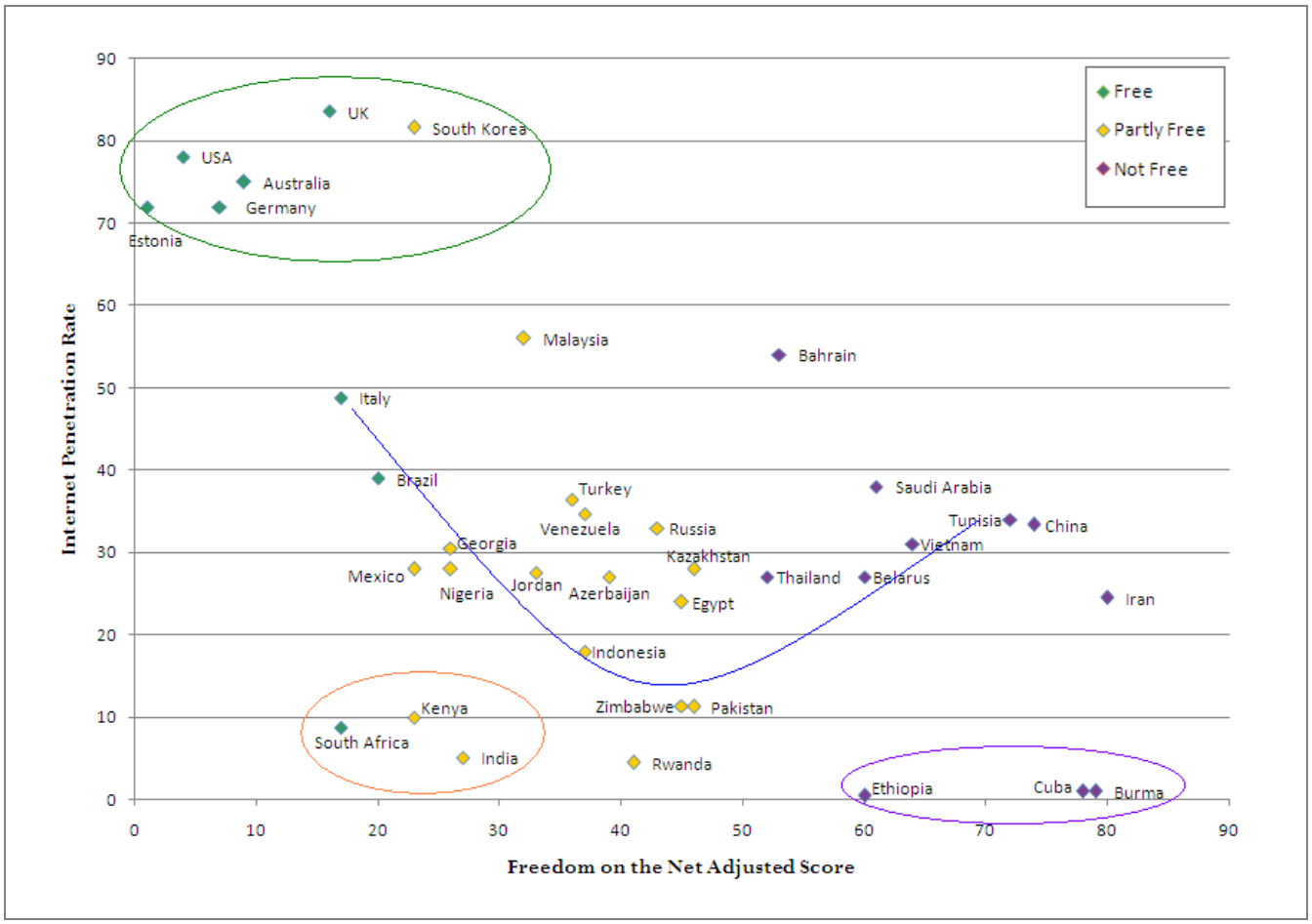


* The front-row bar reflects a country's *Freedom on the Net 2011* score; the back-row bar reflects the country's score on Freedom House's *Freedom of the Press* 2010 index, which primarily assesses television, radio, print media. A green-colored bar represents a status of **"Free,"** a yellow-colored bar represents a status of **"Partly Free,"** while a purple one, the status of **"Not Free."**

INTERNET FREEDOM VS. INTERNET PENETRATION

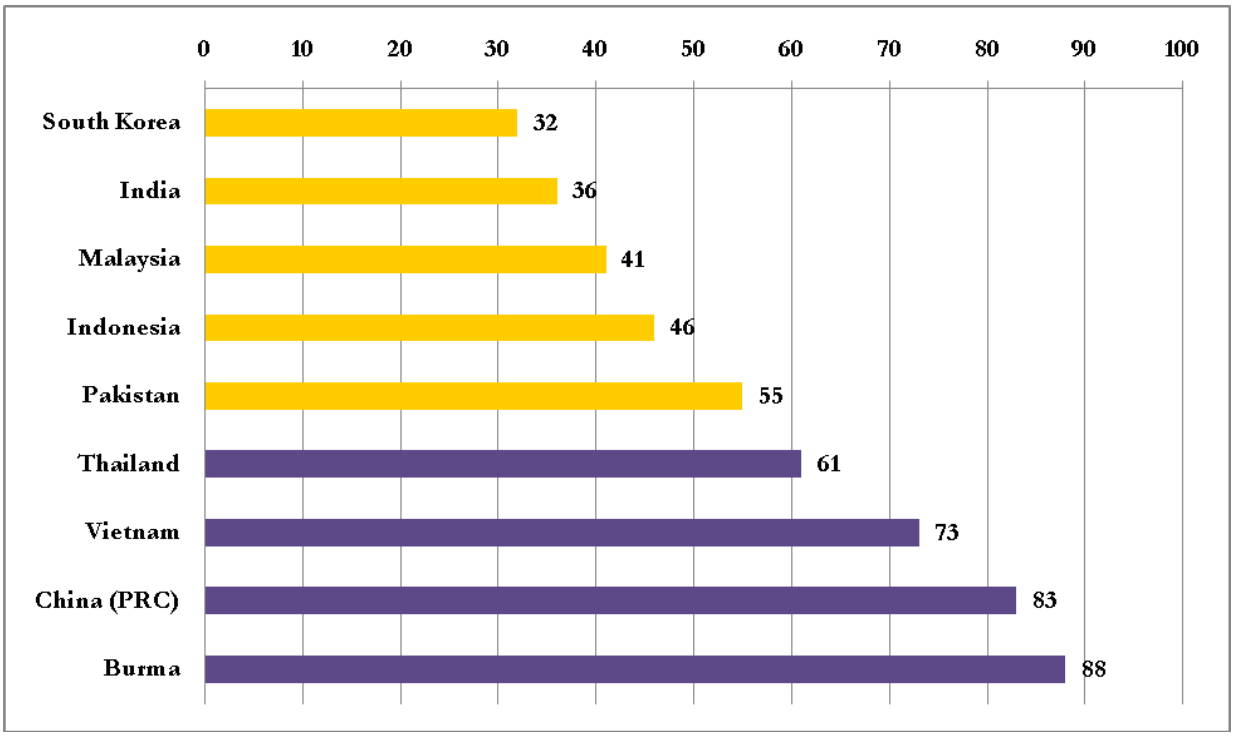
The figure below depicts the relationship between internet penetration rates and the level of digital media freedom as assessed by the *Freedom on the Net 2011* study. Each point is plotted to reflect its level of internet penetration as noted in the report, as well as its performance in the survey. To minimize possible overlap among variables, the scores have been adjusted to exclude performance on the first two questions of the *Freedom on the Net* methodology, which assess the degree of internet access in a given society.

The resulting graph points to several typologies: A cluster of economically developed democratic states with high penetration rates and relatively high levels of internet freedom **(green circle)**; A cluster of lower income democratic states, with relatively lower penetration rates but limited restrictions on other aspects of internet freedom **(orange circle)**; A cluster of lower income authoritarian states, with almost no internet access, as well as heavy restrictions on other aspects of internet freedom **(purple circle)**; A number of states with middling levels of internet penetration and a range of performance on internet freedom. Of note is a potential trajectory for the Partly Free countries in the middle, which may move towards greater repression (the high-tech, Not Free countries on the right) or better protection of free expression (the mid-penetration, Free countries on the left) as penetration rates increase **(blue V pattern)**.

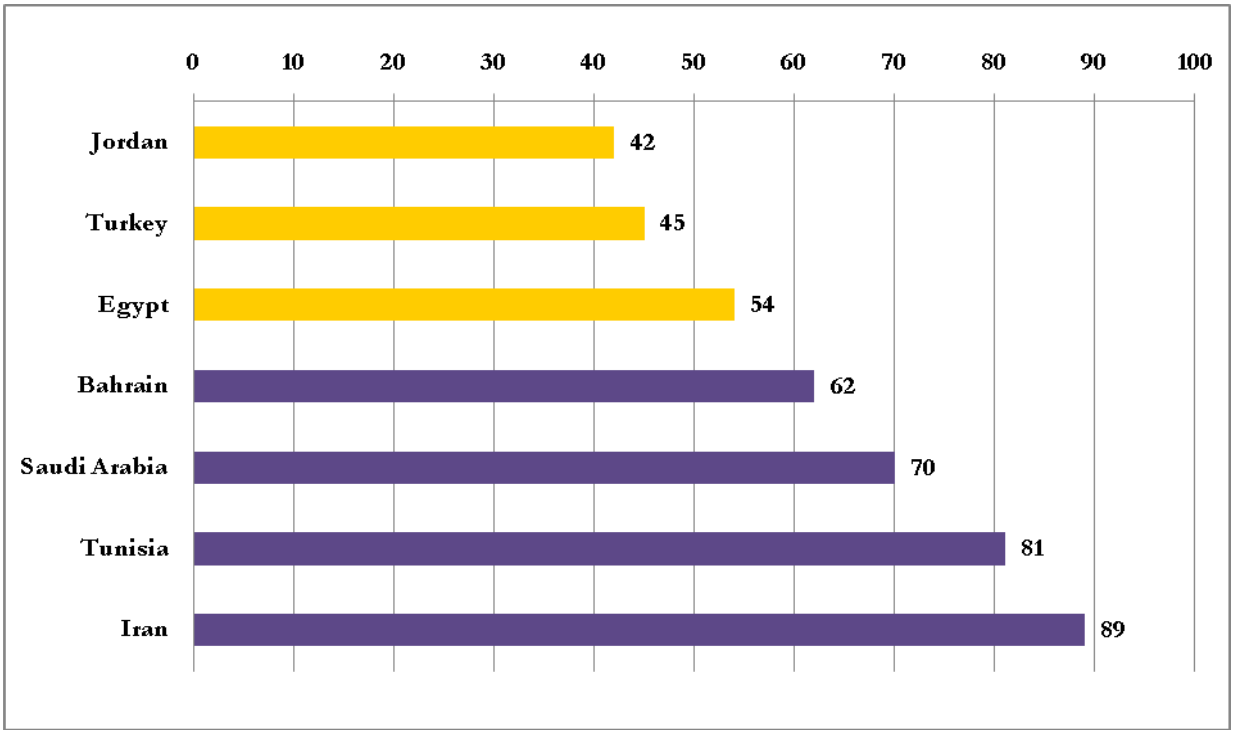


REGIONAL GRAPHS

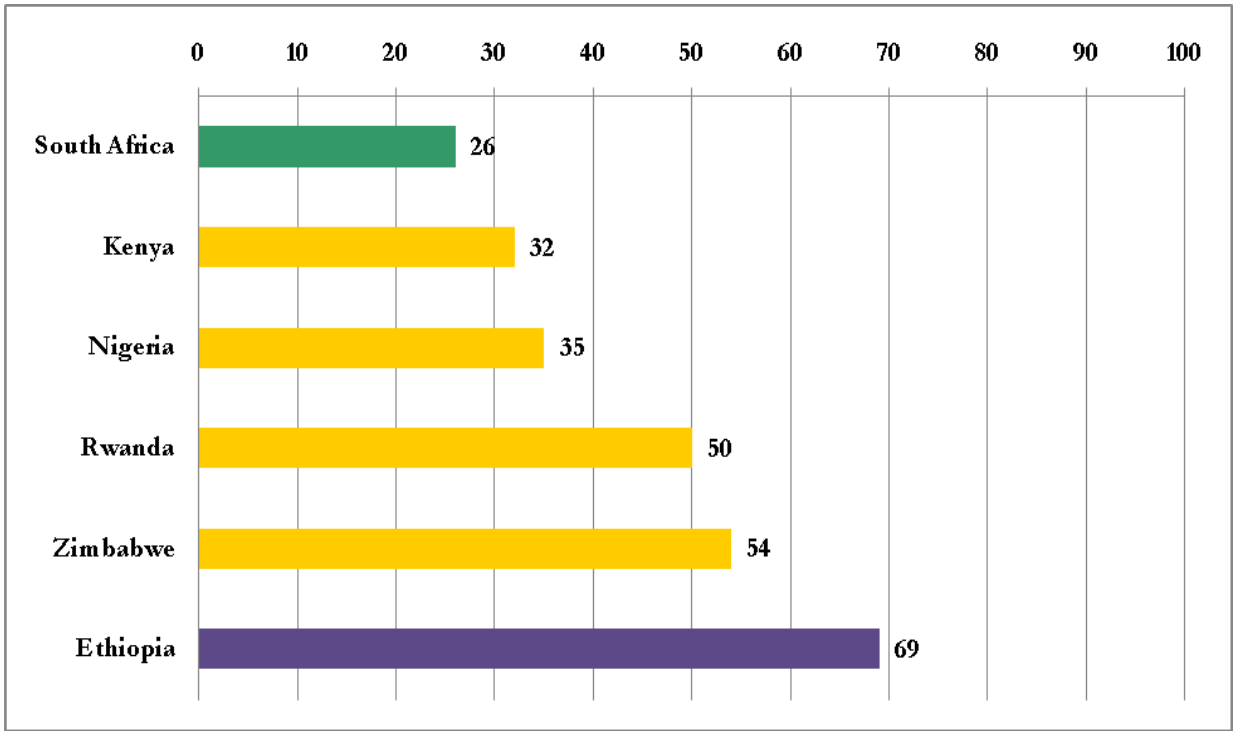
ASIA (0 best, 100 worst)



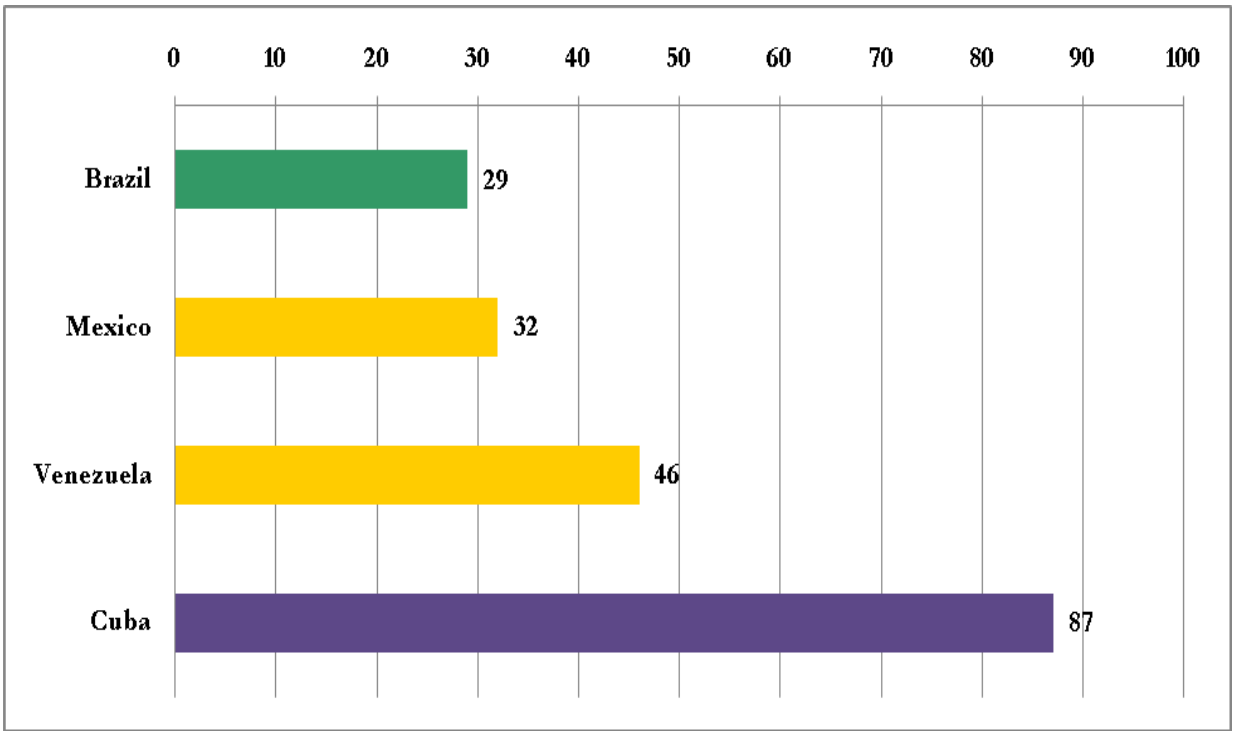
MIDDLE EAST & NORTH AFRICA (0 best, 100 worst)



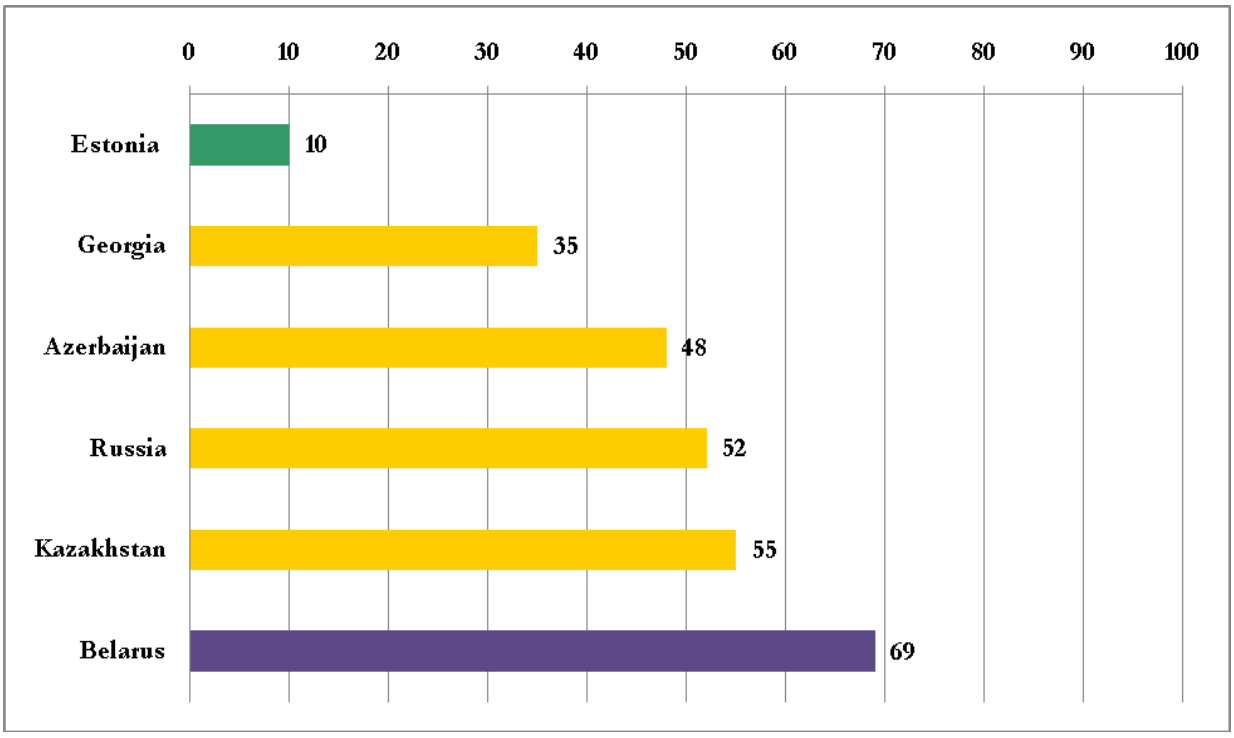
SUB-SAHARAN AFRICA (0 best, 100 worst)



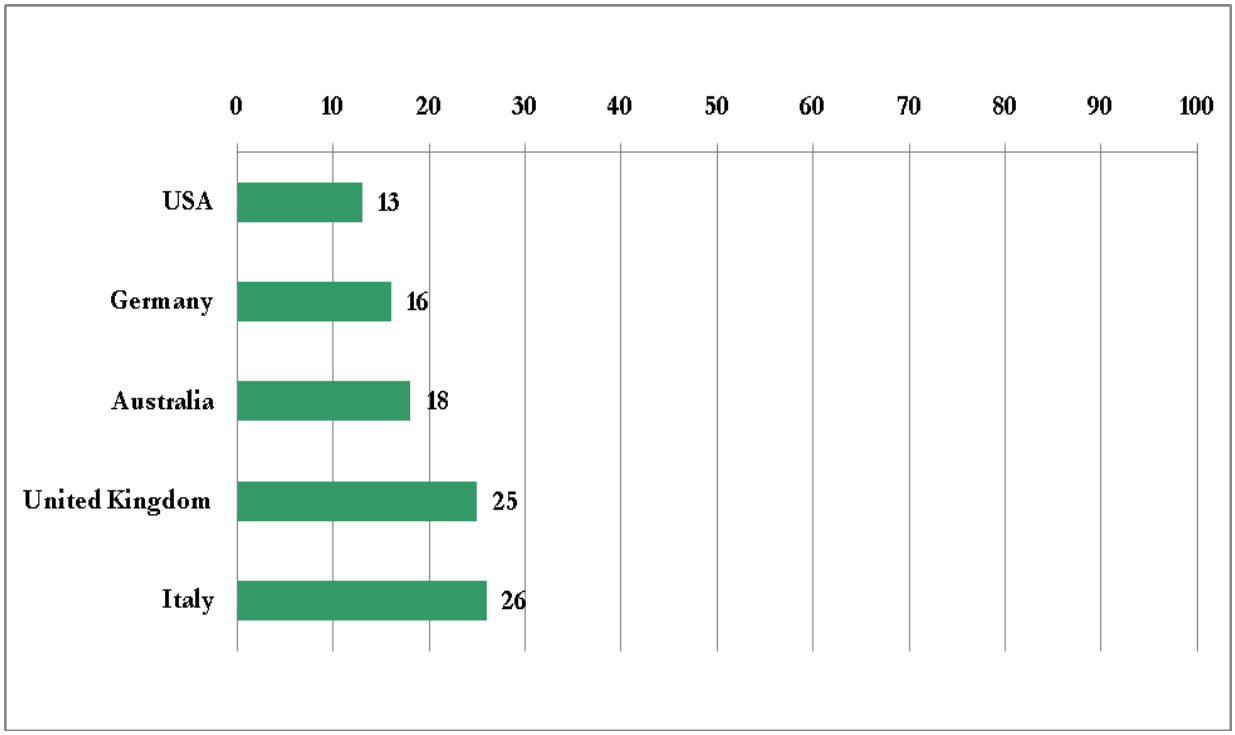
LATIN AMERICA (0 best, 100 worst)



FORMER SOVIET UNION (0 best, 100 worst)

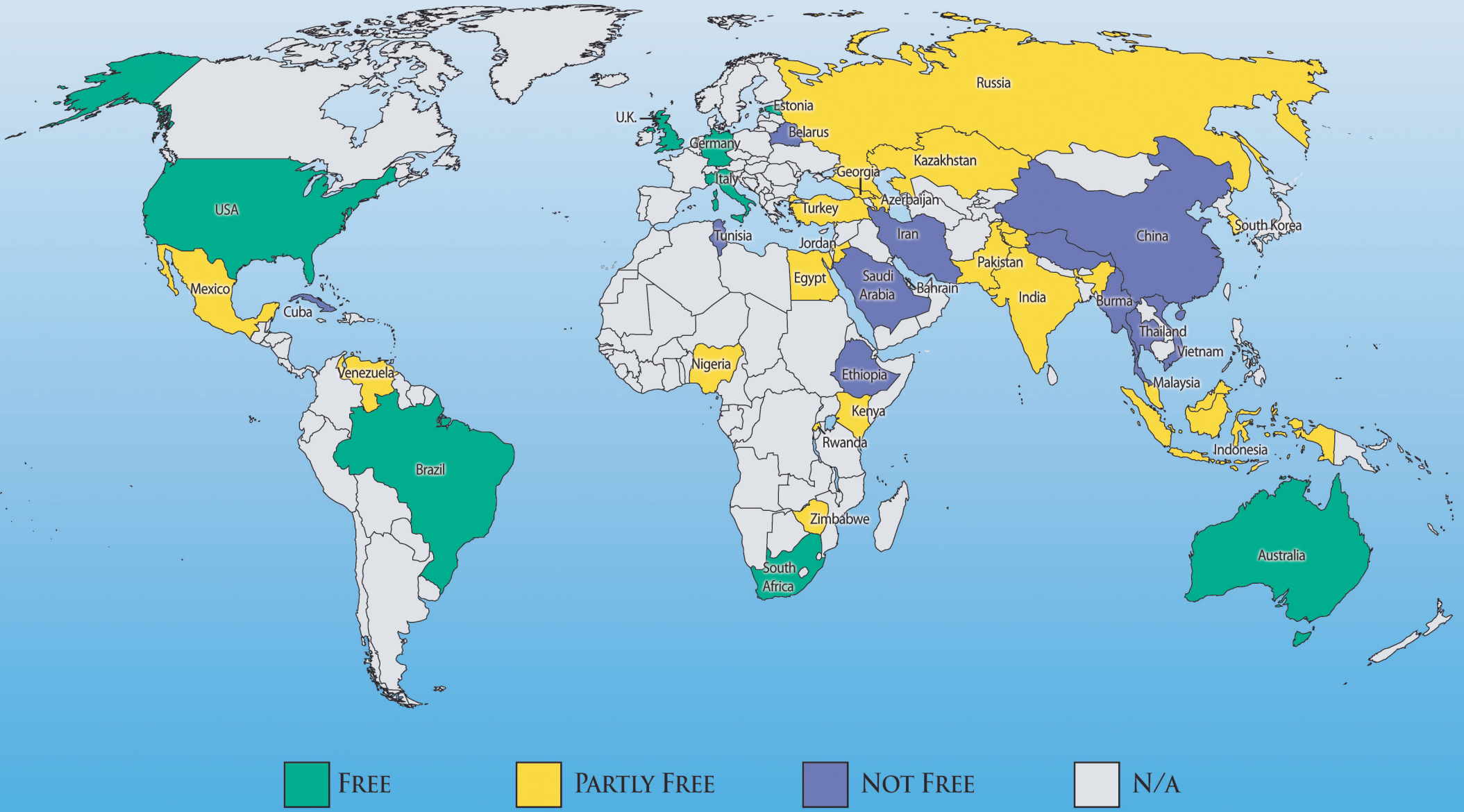


WESTERN EUROPE & OTHERS (0 best, 100 worst)



Freedom on the Net 2011

A Global Assessment of Internet and Digital Media



SCORE CHANGES AND EXPLANATIONS

Among the 37 countries covered in *Freedom on the Net 2011* are all 15 states that were assessed in the 2009 edition of the report. The following are explanations for score improvements and declines in this set of countries. For additional information, see individual Country Reports.

BRAZIL

Freedom on the Net 2009: 30 (Free)
Freedom on the Net 2011: 29 (Free)
Trajectory: Slight improvement

For a country with large social and economic disparities, Brazil has made significant gains in expanding internet access and mobile-phone usage. In recent years, access to the internet further improved, and the total number of users was the fourth largest in the world by 2009. Civic participation through internet media has correspondingly increased and restrictions on political campaigning via social-networking websites imposed ahead of the 2008 elections were removed for the run-up to the 2010 polls. Unlike in previous years, there were no instances of blocks on advanced web applications such as YouTube or the social-networking platform Orkut. These positive developments were slightly offset, however, by several legal and judicial actions that threatened free online expression, including cases of individual bloggers facing unreasonable defamation lawsuits, sometimes for very high amounts. Also noted was the impact of cyberattacks, as several prominent intelligence sources confirmed that a series of attacks in January 2005, September 2007, and November 2009 were responsible for blackouts.

CHINA

***Freedom on the Net 2009*: 79 (Not Free)
***Freedom on the Net 2011*: 83 (Not Free)
Trajectory: Notable decline

Although China is home to the world's largest population of internet users—numbering 446 million by the end of 2010—the country's internet environment remains one of the world's most restrictive, characterized by a sophisticated, multilayered control apparatus. In 2009 and 2010, this system was further enhanced, institutionalized, and decentralized. Blocks on international applications like Facebook and the Twitter became permanent, while censorship requirements on domestic alternatives were enhanced. The authorities also imposed a months-long shutdown of internet access in the western region of Xinjiang. By the end of 2010, the Chinese internet increasingly resembled an intranet. Many average users, isolated from international social media platforms and primarily exposed to a manipulated online information landscape, had limited knowledge of key events related to their own country, even when these make headlines around the world, a dynamic evident with the 2010 awarding of the Nobel Peace Prize to Chinese dissident Liu Xiaobo. In addition, the space for anonymous communication shrank and at least 70 people were in jail for internet-related reasons as of mid-2010, though the actual number of detainees is likely much higher. Tibetans, Uighurs, and Falun Gong practitioners are subject to especially harsh punishments for online activities, and two Uighurs were sentenced to life imprisonment. More than in previous years, China emerged as a key global source of cyberattacks, with targets ranging from groups reporting on Chinese human rights abuses to international financial, defense, and technology companies. The above restrictions were offset somewhat by the internet's continued growth as a primary source of news, a forum for discussion, and a mobilization channel

for many Chinese. Netizens successfully used it to challenge official misconduct, protest censorship, organize strikes, and obtain justice for ordinary citizens, while tech-savvy users employed circumvention tools to access banned sites, such as Twitter.

CUBA

***Freedom on the Net 2009*: 88 (Not Free)**
***Freedom on the Net 2011*: 87 (Not Free)**
Trajectory: Slight improvement

Cuba remains one of the world's most repressive environments for the internet and other information and communication technologies (ICTs). There is almost no access to internet applications other than e-mail, and surveillance is extensive, with special software employed to monitor and control many of the island's public internet-access points. Nevertheless, in recent years there has been a slight loosening of restrictions on the sale of computers, and important growth of mobile-phone infrastructure was evident in 2009. In addition, despite the threat of detention and travel restrictions, a community of bloggers has consolidated their work, creatively using online and offline means to express opinions and spread information about conditions in the country. Cuba still has the lowest mobile-phone penetration rate in Latin America, however, and most users continue to face extremely slow connections, making the use of multimedia applications nearly impossible.

EGYPT

***Freedom on the Net 2009*: 51 (Partly Free)**
***Freedom on the Net 2011*: 54 (Partly Free)**
Trajectory: Notable decline

While the Egyptian government has aggressively and successfully sought to expand access to the internet as an engine of economic growth, its security forces also intensified attempts to curtail the use of new technologies for disseminating and receiving sensitive political information in 2009 and 2010. They typically employ such "low-tech" methods as intimidation, legal harassment, detentions, and real-world surveillance of online dissidents. However, in response to increased internet-based activism, particularly in advance of the November 2010 parliamentary elections, the authorities began to engage in greater censorship of online communications. Several individuals who called for political change and democratic reform saw their websites shut down and two popular Facebook groups used for organizing protests were temporarily removed. With Emergency Law provisions in place, Egypt's legal environment remained harsh and several bloggers were detained during the coverage period, with one nearly tried before a military tribunal. In 2010, Egypt also saw the first court case in which a judge found a cybercafe owner liable for defamatory information posted online by a visitor to his shop.

ESTONIA

***Freedom on the Net 2009*: 13 (Free)**
***Freedom on the Net 2011*: 10 (Free)**
Trajectory: Notable improvement

Estonia ranks among the most wired and technologically advanced countries in the world. In 2009, over 91 percent of citizens filed their taxes online and Estonian identity cards were used to facilitate electronic voting during municipal and European Parliament elections. Restrictions on internet content and communications are among the lightest in the world. Nevertheless, in January 2010, a new law on online gambling came into force, requiring all domestic and foreign gambling sites to

obtain a special license or face access restrictions. The most serious threat to internet freedom in Estonia emerged in late April and early May 2007, when a campaign of cyberattacks targeted various Estonian institutions and infrastructures. Given the absence of such a large-scale attack in 2009-2010, and the subsequent restrictions it posed for access to important information, Estonia's score showed improvement during the coverage period. In addition, the experience led to increased awareness of the dangers of cyberattacks and a greater policy focus on improving technical competencies to make the internet more secure.

GEORGIA

***Freedom on the Net 2009*:** 43 (Partly Free)
***Freedom on the Net 2011*:** 35 (Partly Free)
Trajectory: Significant improvement

Use of the internet and related technologies has grown rapidly in Georgia in recent years, with internet penetration surpassing the 30 percent mark in 2009, partly the result of lower prices. There were no reports of government censorship during the coverage period and users were able to freely visit any website around the world, including advanced web applications. This was in contrast to the period in August 2008, during a brief military conflict with Russia, when the government blocked access to all Russian addresses (those using the .ru country code), including the popular blogging service LiveJournal. The filtering was eased within days and did not resurface. This change contributed to Georgia's score improvement, along with the absence of large-scale cyberattacks by Russian hackers that also featured in the 2008 conflict. Some restrictions on internet freedom did occur in 2009 and 2010, however. In November 2009, two young students were detained after allegedly insulting the widely respected head of the Georgian Orthodox Church in videos posted on YouTube. In addition, some online media outlets reported instances of advertisers deciding to withdraw ads after the outlet published news articles overly critical of the government.

INDIA

***Freedom on the Net 2009*:** 34 (Partly Free)
***Freedom on the Net 2011*:** 36 (Partly Free)
Trajectory: Slight decline

Although India's internet penetration rate of less than 10 percent is low by global standards, access has expanded rapidly in urban areas, generating tens of millions of new users in recent years. In the past, instances of the central government seeking to control communication technologies were relatively rare. However, following the November 2008 terrorist attacks in Mumbai and with an expanding Maoist insurgency, the need, desire, and ability of the Indian government to control the communications sector have grown. In 2008, Parliament passed amendments to the Information Technology Act (ITA), which came into effect in 2009 and have expanded the government's monitoring capabilities. Pressure has also increased on private intermediaries to remove certain information. Though most requests have targeted comments that might incite communal violence, some observers have raised concerns of certain removals being unnecessary. The fairness of bidding processes surrounding the allocation of ICT resources also came into question in 2010 with the exposure of a major corruption scandal involving the licensing of second-generation (2G) mobile-phone services.

IRAN

***Freedom on the Net 2009*: 76 (Not Free)**
***Freedom on the Net 2011*: 89 (Not Free)**
Trajectory: Significant decline

Iran showed the greatest decline among the countries surveyed, placing it as the worst performer in this edition. Since the protests that followed disputed presidential elections in June 2009, the Iranian authorities have waged an active campaign against internet freedom, employing extensive and sophisticated methods of control that go well beyond simple content filtering, though this too has become more severe since the election. Tactics employed include deliberately slowing internet speeds at critical times to make basic online activities difficult and ordering blogging service providers inside Iran to remove "offensive" posts. The regime has also sought to counter critical content and online organizing efforts by extending state propaganda into the digital sphere: over 400 news websites are either directly or indirectly supported by the state. Since June 2009, an increasing number of bloggers have been threatened, arrested, tortured, and kept in solitary confinement, and at least one blogger died in custody. Over 50 bloggers and online activists have been arrested, and a dozen remained in detention at the end of 2010. The Iranian authorities have taken a range of measures to monitor online communications, and a number of protesters who were put on trial after the election were indicted for their activities on Facebook and Balatarin, a Persian site that allows users to share links and news. A group calling itself the Iranian Cyber Army, later found to be associated with the Iranian authorities, also managed to hack a number of opposition and news sites with a mix of technical methods and forgery.

KENYA

***Freedom on the Net 2009*: 34 (Partly Free)**
***Freedom on the Net 2011*: 32 (Partly Free)**
Trajectory: Slight improvement

Although a lack of infrastructure and high costs still hamper connectivity for many Kenyans, the installation of two undersea cables in 2009 dramatically improved bandwidth to 13 times the speed from the previous year. Since 2008, there have been no confirmed incidents of government filtering or interference with online communication, despite earlier fears that the authorities might seek to impose greater controls after the internet was used as a channel for spreading hate speech during election-related violence. In January 2009, the government passed a controversial Communications Amendment Act, ignoring warnings from civil society that it could hinder free expression.

MALAYSIA

***Freedom on the Net 2009*: 41 (Partly Free)**
***Freedom on the Net 2011*: 41 (Partly Free)**
Trajectory: No change

By 2009, over 55 percent of the total population in Malaysia accessed the internet. In the watershed general elections of March 2008, the ruling National Front (BN) coalition lost its two-thirds parliamentary majority for the first time since 1969. The use of the internet for political mobilization and news dissemination was widely seen as contributing to the opposition's electoral gains. In both the run-up to and aftermath of the elections, many observers sensed that the government and ruling coalition had recognized the potential political impact of the internet and had therefore grown more determined to control it. Throughout 2009 and 2010, a number of bloggers faced legal harassment,

intimidation, fines, and brief periods of detention, though none were imprisoned. Many of these cases involve individuals who had been critical of Malaysian royalty, while others were detained over satirical content. The government also made a more concerted effort to influence public opinion by establishing its own presence online and several online news outlets and opposition-related websites faced cyberattacks. However, more systemic forms of censorship, such as technical filtering, were not implemented.

RUSSIA

***Freedom on the Net 2009*:** 49 (Partly Free)
***Freedom on the Net 2011*:** 52 (Partly Free)
Trajectory: Notable decline

With the tightening of traditional media controls since 2000, the internet has become Russia's last relatively uncensored platform for public debate. However, even as access conditions have improved, internet freedom has corroded. In the last two years, the country's first high-profile cases of technical blocking were reported, while tactics for proactively manipulating conversations in the online sphere were refined. Regional blocking, whereby a website is blocked in some areas but remains available elsewhere in the country, was particularly evident. In one example of the phenomenon, a regional network provider in December 2010 temporarily blocked users from accessing an environmentalist website, allegedly because the site initiated a petition to dismiss a local mayor. Russian bloggers also faced increasing intimidation: at least 25 cases of blogger harassment by the authorities occurred in 2009 and 2010, including 11 arrests. In addition, several newspaper websites experienced cyberattacks, typically in connection with articles that could seriously influence offline events. At least 16 blogs suffered hacking attacks during the coverage period.

SOUTH AFRICA

***Freedom on the Net 2009*:** 24 (Free)
***Freedom on the Net 2011*:** 26 (Free)
Trajectory: Slight decline

Digital media freedom continues to be respected in South Africa. Access to the internet has improved, with more people having an option to access the internet from their mobile telephones than from computers, though the majority of the population is unable to benefit from internet access. While internet content remains largely free of government censorship, a recent amendment to the Films and Publications Act of 1996 has raised fears that controversial content could be restricted. The amendment, which was passed into law in 2009, requires that every print and online publication that is not a recognized newspaper be submitted for classification to the government-controlled Film and Publications Board if it includes depictions of sexual or disrespectful content. Other areas of concern include lack of parliamentary oversight in relation to interception orders and lack of transparency surrounding take-down notices, though there were no known instances of such requests targeting politically relevant content.

TUNISIA

***Freedom on the Net 2009*:** 76 (Not Free)
***Freedom on the Net 2011*:** 81 (Not Free)
Trajectory: Notable decline

Since the government tightly controls traditional media, the internet has emerged as a comparatively open forum for airing political and social opinions. As internet penetration grew, reaching 34 percent of the population by 2009, the regime of former President Ben Ali

responded by creating a multilayered censorship apparatus that was among the world's most sophisticated. Despite an already robust system in place, in 2009 and especially in 2010, censorship expanded and became increasingly arbitrary. Several human rights activists and online journalists were arbitrarily detained, monitored and harassed, while websites were subject to targeted technical attacks, sometimes causing deletion of large amounts of content. Conditions further deteriorated after an unemployed fruit vendor set himself on fire in later December 2010 to protest joblessness, sparking country-wide protests, along with calls for political reform and greater employment opportunities. Social media sites such as Twitter, YouTube, and Facebook, as well as various blogs, played an important role in providing independent information and analysis, spreading the protesters' demands, and showing videos of demonstrations across the country. This, in turn, resulted in the government's increased efforts to dismantle networks of online activists, hack into their social networking and blogging accounts, conduct extensive online surveillance, and disable activists' online profiles and blogs.

TURKEY

***Freedom on the Net 2009*: 42 (Partly Free)**
***Freedom on the Net 2011*: 45 (Partly Free)**
Trajectory: Notable decline

Internet and mobile-telephone use in Turkey has grown significantly in recent years, surpassing one third of the population in 2009, though access remains a challenge in some parts of the country. Since 2001, the government has taken considerable legal steps to limit access to certain information, including some political content. According to various estimates, there were over 5,000 blocked websites as of July 2010, an increase from 2008, spurring street demonstrations against internet censorship. In addition, certain applications, particularly file-sharing sites like YouTube, Last.fm, and Metacafe, as well as some Google-related services, have been repeatedly blocked. The YouTube block was eventually lifted in November 2010, but only after disputed videos were removed or made unavailable within the country. Despite a restrictive legal environment, the Turkish blogosphere is vibrant and diverse. Bloggers have critiqued even sensitive government policies and sought to raise public awareness about censorship and surveillance practices, yielding at least one parliamentary inquiry into the latter.

UNITED KINGDOM

***Freedom on the Net 2009*: 23 (Free)**
***Freedom on the Net 2011*: 25 (Free)**
Trajectory: Slight decline

The United Kingdom has high levels of internet penetration, and online free expression is generally respected. However, both the government and private parties have presented challenges to free speech in connection with antiterrorism efforts, public order, and intellectual property. The biggest recent controversy was the adoption of the Digital Economy Act in April 2010. The law allows for the blocking of websites and the cutting off of user accounts based on claims of intellectual-property rights violations. Free expression advocates also complain that procedures for blocking and removing content related to pornography and terrorism are not transparent, clear, or supported by an adequate appeals process. In efforts to combat terrorism, the government has taken measures against users who post or download information perceived as a security threat, including one case of a man convicted for using Twitter to express dismay at the closing of a local airport and writing that he would blow up the airport if it did not reopen within a week. The newly elected coalition government has promised to review and repeal a number of laws that negatively affect online rights, including expansively interpreted libel laws.

COUNTRY REPORTS

AUSTRALIA

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Free**
Obstacles to Access	n/a	3
Limits on Content	n/a	6
Violations of User Rights	n/a	9
Total	**n/a**	**18**

POPULATION: 22 million
INTERNET PENETRATION 2009: 75 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Free

INTRODUCTION

Although Australia enjoys affordable, high-quality access to the internet and other digital media, recent amendments to surveillance legislation and proposals to implement censorship through directives to internet-service providers (ISPs) have raised concerns about privacy and freedom of expression.[1] Draft legislation was proposed in 2010 that would require ISPs to filter illicit content and retain data on users' online activities. However, following the election of a new government, as of December 2010, these plans had been put on hold.

In 1989, Australia's Research and Education Network (AARNet) made the first internet connection with a 56 kilobit per second satellite link between the University of Melbourne and the University of Hawaii.[2] Today, the same connection to the United States is 200,000 times faster, and with the development of the high-speed National Broadband Network (NBN), all Australians, including those in more remote areas, will soon enjoy connection speeds near 100 megabits per second.[3] There were over 9.1 million active

[1] For a comprehensive overview of the legislative history of censorship in Australia *see* Libertus.net, "Australia's Internet Censorship System," http://libertus.net/censor/netcensor.html, accessed June 2010. *See also* Australian Privacy Foundation, http://privacy.org.au, accessed June 2010.

[2] Australia's Research and Education Network (AARNet), "AARNet Salutes the 20th Anniversary of the Internet in Australia," news release, November 26, 2009, http://www.aarnet.edu.au/Article/NewsDetail.aspx?id=173; Roger Clarke, "A Brief History of the Internet in Australia," May 5, 2001, http://www.rogerclarke.com/II/OzIHist.html; Roger Clarke, "Origins and Nature of the Internet in Australia," January 29, 2004, http://www.rogerclarke.com/II/OzI04.html.

[3] Australian Government, Department of Broadband, Communications and the Digital Economy, "National Broadband Network," http://www.dbcde.gov.au/broadband/national_broadband_network, accessed June 2010.

internet subscribers in Australia at the end of 2009 and nearly 16 million internet users, a penetration rate of approximately 75 percent.[4]

OBSTACLES TO ACCESS

Access to the internet and other digital media in Australia is widespread, almost ubiquitous. Australians have a number of internet connection options, including ADSL, ADSL 2+, wireless, cable, satellite, and dial-up.[5] Wireless systems can reach 99 percent of the population, while satellite capabilities are able to reach 100 percent. The phasing out of dial-up continues, with nearly 90 percent of internet connections now provided through other means. Once implemented, the NBN will eliminate the need for any remaining dial-up connections and make high-speed broadband available to Australians in remote and rural areas.[6]

In 2008, approximately 73 percent of people aged 14 and over lived in a household with an internet connection, while 58 percent lived in a household with a broadband connection.[7] These figures are expected to steadily increase to 100 percent with the implementation of the NBN. Although internet access is widely available in locations such as libraries, educational institutions, and internet cafes, Australians predominantly access the internet from home, work, and increasingly through mobile telephones. The majority of all age groups are using the internet, with the exception of those aged 65 and over.[8] Age is a significant indicator of internet use, with 100 percent of teenagers (aged 14 to 17) reporting that they have used the internet, 92 percent of them to a medium or heavy degree. By contrast, only 56 percent of those aged 65 and over have used the internet, and just 40 percent report heavy or medium usage.[9] Approximately 50 percent of Aboriginal and Torres Strait Islanders living in discrete indigenous communities (not major cities) have access to the internet with 36 percent having internet access in the home.[10]

---

[4] Australian Bureau of Statistics, "Internet Activity, Australia" (June, 2010), http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/ accessed December 30, 2010; International Telecommunications Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

[5] Australian Communications and Media Authority (ACMA), *Communications Report, 2008–09* (Canberra: ACMA, 2009), http://www.acma.gov.au/webwr/_assets/main/lib311252/08-09_comms_report.pdf.

[6] Australian Government National Broadband Network, "NBN Key Questions and Answers" http://www.nbn.gov.au/content/nbn-key-questions-and-answers-faqs accessed June 2010.

[7] ACMA, *Communications Report, 2008–09*.

[8] ACMA, *Australia in the Digital Economy, Report 2: Online Participation* (Canberra: ACMA, 2009), http://www.acma.gov.au/WEB/STANDARD/pc=PC_311655.

[9] Ibid.

[10] Australian Bureau of Statistics, "Internet Access at Home" 2006, http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4102.0Chapter10002008 accessed October 2010. For a

Australia has a mobile-phone penetration rate of 110 percent with many consumers using more than one SIM card or mobile phone.[11] In remote indigenous communities 63 percent of the population had taken up mobile-phone services in 2004.[12] However, not all indigenous communities have mobile-phone coverage such that the overall mobile-phone penetration rate in Aboriginal communities is unknown. Third-generation (3G) mobile services are the driving force behind the recent growth, with 12.28 million 3G mobile subscriptions operating as of June 2009.[13]

Internet access is affordable for most Australians. The government subsidizes satellite phones and internet connections for individuals and small businesses in remote and rural areas, where internet access is not comparable to that in metropolitan areas.[14]

Australia, like most other industrialized nations, hosts a competitive market for internet access, with 104 medium- to large-sized ISPs and another 585 small providers. Many of the latter are "virtual" maintaining only a retail presence and offering end users access through the network facilities of other companies.[15] ISPs are considered carriage-service providers under Australian law. As such they are required to obtain a license from the Australian Communications and Media Authority (ACMA) and submit to dispute resolution by the Telecommunications Industry Ombudsman (TIO). Australian ISPs are co-regulated under Schedule 7 of the 1992 Broadcasting Services Act (BSA), meaning there is a combination of regulation by the ACMA and self-regulation by the telecommunications industry.[16] The industry's involvement consists of the development of industry standards and codes of practice.

The government has adopted a strong policy of technical neutrality. There are no limits to the amount of bandwidth that ISPs can supply. While the government does not place restrictions on bandwidth, ISPs are free to adopt internal market practices on traffic shaping. Some Australian ISPs practice traffic shaping under what are known as fair-use policies. If a customer is a heavy peer-to-peer user, the internet connectivity for those activities will be slowed down to free bandwidth for other applications.[17] Advanced web applications like the social-networking sites Facebook and MySpace, the Skype voice-

comprehensive report on indigenous Internet use and access *see* ACMA, *Telecommunications in Remote Indigenous Communities* (Canberra: ACMA, 2008), page 48, http://www.acma.gov.au/WEB/STANDARD/pc=PC_311397 accessed June 2010.

[11] ACMA, *Communications Report, 2008-09*.

[12] ACMA, *Telecommunications in Remote Indigenous Communities*, page 30-32.

[13] ACMA, *Communications Report, 2008-09*.

[14] Rural Broadband, "Welcome," http://www.ruralbroadband.com.au, accessed June 2010.

[15] Australian Bureau of Statistics, "Internet Activity, Australia, Dec 2009," http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8153.0Main+Features1Dec%202009?OpenDocument.

[16] Australian Communications and Media Authority Act 2005, http://www.austlii.edu.au/au/legis/cth/consol_act/acamaa2005453/; Broadcasting Services Act 1992, http://www.austlii.edu.au/au/legis/cth/consol_act/bsa1992214/; ACMA, "Service Provider Responsibilities," http://www.acma.gov.au/WEB/STANDARD/1001/pc=PC_90157, accessed June 2010.

[17] Vuze, "Bad ISPs," http://wiki.vuze.com/w/Bad_ISPs#Australia, accessed June 2010.

communications system, and the video-sharing site YouTube are neither restricted nor blocked in Australia.

The ACMA is the primary regulator for the internet and mobile telephony, and is responsible for enforcing Australia's anti-spam law.[18] Its oversight is generally viewed as fair and independent, though there are some transparency concerns with regard to classification of content. Small businesses and residential customers may file complaints about internet, telephone, and mobile-phone services with the Telecommunications Industry Ombudsman (TIO),[19] which operates as a free and independent dispute-resolution scheme.

LIMITS ON CONTENT

Australian law does not currently provide for mandatory blocking or filtering of websites, blogs, chat rooms, or platforms for peer-to-peer file sharing. Access to online content is far-reaching, and Australians are able to explore all facets of political and societal discourse, including information about human rights violations. Their ability to openly express dissatisfaction with politicians and to criticize government policies is not hindered by the authorities.[20]

However, there are two regimes that regulate internet content. Under one regime, material deemed by the ACMA to be "prohibited content" is subject to take-down notices. The relevant ISP is notified by the ACMA that it is hosting illicit content, and it is then required to take down the offending material.[21] Under the BSA, the following categories of online content are prohibited:

- Any online content that is classified Refused Classification (RC) by the Classification Board, including real depictions of actual sexual activity; child pornography; depictions of bestiality; material containing excessive violence or sexual violence; detailed instruction in crime, violence, or drug use; and material that advocates the commission of a terrorist act.

[18] ACMA, "The ACMA Overview," http://www.acma.gov.au/WEB/STANDARD/pc=ACMA_ORG_OVIEW, accessed June 2010;
ACMA, "How Regulation Works," http://www.acma.gov.au/WEB/STANDARD/pc=PUB_REG_ABOUT, accessed June 2010.

[19] Telecommunications Industry Ombudsman, http://www.tio.com.au, accessed June 2010.

[20] Chris Nash, "Freedom of the Press in Australia," Democratic Audit of Australia, November 19, 2003, http://democratic.audit.anu.edu.au/papers/20031119_nash_press_freed.pdf.

[21] Internet Society of Australia, "Who Is an Internet Content Host or an Internet Service Provider (and How Is the ABA Going to Notify Them?," http://www.isoc-au.org.au/Regulation/WhoisISP.html, accessed June 2010;
Stuart Corner, "EFA Fights ACMA Over 'Take-Down' Notice," iTWire, April 20, 2010, http://www.itwire.com/it-policy-news/regulation/38423-efa-fights-acma-over-take-down-notice; Internet Industry Association, "Guide for Internet Users," March 23, 2008, http://www.iia.net.au/index.php/initiatives/guide-for-users.html.

- Content that is classified R 18+ and not subject to a restricted access system that prevents access by children, including depictions of simulated sexual activity; material containing strong, realistic violence; and other material dealing with intense adult themes.
- Content that is classified MA 15+, provided by a mobile premium service or a service that provides audio or video content upon payment of a fee and that is not subject to a restricted access system, including material containing strong depictions of nudity, implied sexual activity, drug use, or violence; very frequent or very strong coarse language; and other material that is strong in impact.[22]

To date, this system for restricting access to videos, films, literature and similar material via take-down notices has not emerged as problematic in terms of any overflow to information of political or social consequence. In addition, the general disposition is to allow adults unfettered access to R 18+ materials while protecting children from exposure to inappropriate content.

Under the second regime, the ACMA may direct an ISP or content service provider to comply with the Code of Practice developed by the Australian Internet Industry Association (IIA) if the regulator decides that it is not already doing so. Failure to comply with such instructions may draw a maximum penalty of A$11,000 (US$10,800) per day. Other regulatory measures require ISPs to offer their customers a family-friendly filtering service.[23] This is known as voluntary filtering, as customers must select it as an option.

However, in recent years, the government has proposed implementing a mandatory filtering system run through ISPs.[24] Draft legislation was proposed under the Labor government led by Kevin Rudd, but was then put aside in the run-up to elections held in August 2010. Under the previously proposed draft, the list of sites to be blocked would initially focus on images of child abuse, particularly child pornography. The ACMA would have the responsibility of maintaining the blacklist, but the criteria for blocking sites remained nebulous. Under the latest proposal, the ACMA would blacklist any content classified as RC, and its early trials of internet filters used an initial list of over 1,300 sites, versions of which were leaked.[25] The list revealed that the overwhelming majority of

[22] ACMA, "Prohibited Online Content," http://www.acma.gov.au/WEB/STANDARD/pc=PC_90102, accessed June 2010.
[23] Internet Industry Association (IIA), *Internet Industry Code of Practice: Content Services Code for Industry Co-Regulation in the Area of Content Services (Pursuant to the Requirements of Schedule 7 of the Broadcasting Services Act 1992), Version 1.0*, 2008, http://www.iia.net.au/images/content_services_code_registration_version_1.0.pdf.
[24] Alana Maurushat, Renee Watt, "Australia's Internet Filtering Proposal in the International Context," *Internet Law Bulletin* 12, no. 2 (2009); ACMA, "Internet Service Provider Filtering," http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering.
[25] ACMA, "Internet Service Provider Filtering"; Wikileaks, "Australian Government Secret ACMA Internet Censorship Blacklist, 18 Mar 2009," http://mirror.wikileaks.info/wiki/Australian_government_secret_ACMA_internet_censorship_blacklist,_18_Mar_2009/, accessed February 2011.

websites hosted child pornography. However, there were a few notable exceptions of a gambling site, a euthanasia site, and a few pornography and fetish sites that did not host child pornography. The list, therefore, contained both banned content that it was designed to block and broader content that many would consider reasonable to remain accessible, fueling public fears that the system could be easily abused to expand censorship.

The proposed filtering system has been controversial in Australia as there are concerns of over-blocking, censorship of adult materials, scope creep, and impairment of telecommunication access speeds.[26] The federal elections in August 2010 saw the forming of a minority government with Julia Gillard of the Labor Party coming to power. While Gillard has voiced support for the filter in the media, the likelihood of any such proposal becoming law is slim due to the strong opposition to any such legislation by opposition parties.[27] Therefore, as of December 2010, the status of the initiative remained ambiguous and no internet filtering bill had been introduced in Parliament.

RC content, including many forms of adult pornography, is generally not unlawful to use, access, possess, or create in Australia merely by virtue of its RC status. Only material that is otherwise legislatively criminalized, such as material depicting child abuse and certain terrorism-related content, is unlawful. Moreover, Australia has no X 18+ or R 18+ category for video and computer games. This means that extremely violent video games beyond the MA 15+ classification level are necessarily categorised as RC.[28] The lack of a R +18 classification for video games has led to some peculiar results with games such as *Aliens vs Predators* initially given an RC classification which was later amended to M+ 15.[29] When a game is classified as RC often the developer will slightly modify the game to ensure an M+15 ranking.[30]

The currently existing classification system suffers from a lack of transparency, and there is no mechanism available for owners or creators to challenge the classification of RC content, which can be subject to take-down notices or possible blocking in the future by the proposed filter. Only the ISP or similar intermediary hosting the material may bring a challenge to the Administrative Appeals Tribunal (AAT). Australian content owners are not informed by the ACMA if it issues a take-down notice to their host.

---

[26] *See generally* Alana Maurushat and Renee Watt, Australia's Internet filter Proposal in the International Context, Internet Law Bulletin April 2009, page 18-25; and David Vaile and Renee Watt, "Inspecting the Despicable, Assessing the Unacceptable: Prohibited Packets and the Great Firewall of Canberra" (2009) University of New South Wales Law Review Series 35.

[27] The Sydney Morning Herald, "Internet Filter is Right: Gillard" October 12, 2010 http://news.smh.com.au/breaking-news-national/internet-filter-is-right-gillard-20101012-16hiz.html.

[28] Libertus.net, "Australia's Internet Censorship System," http://libertus.net/censor/netcensor.html; Wikileaks, "Australian Government Secret ACMA Internet Censorship Blacklist, 18 Mar 2009."

[29] Australian Government – Classification Review Board 2009, *Alien vs. Predator – Review Board Decision Reasons,* http://www.classification.gov.au/www/cob/rwpattach.nsf/VAP/%28C7C220BBE2D77410637AB17935C2BD2E%29~DecisionReasons-AliensvsPredator-Final-4January2010.pdf/$file/DecisionReasons-AliensvsPredator-Final-4January2010.pdf.

[30] See generally Chalk, OFLC reveals changes to Australian *Fallout 3*, August 13, 2008, http://www.escapistmagazine.com/news/view/85646-OFLC-Reveals-Changes-To-Australian-Fallout-3.

Journalists, commentators, and ordinary users are not subject to censorship so long as their content does not amount to defamation or breach criminal laws, such as those against hate speech or racial vilification.[31] Nevertheless, the need to avoid defamation has been a significant driver of self-censorship by both the media and ordinary users (see "Violations of Users' Rights").

Australians have access to a broad choice of online news sources that express diverse, uncensored political and social viewpoints. Individuals are able to use the internet and other technologies both as sources of information and as tools for mobilization.[32]

Digital media such as blogs, Twitter feeds, Wikipedia pages, and Facebook groups have been harnessed for a wide variety of purposes ranging from elections, to campaigns against government corporate activities, to a channel for safety-related alerts where urgent and immediate updates were required.[33] For instance, Google Maps was used in a creative endeavour to map out fire dissemination in the devastating 2009 wildfires that spread across the State of Victoria.[34]

VIOLATIONS OF USER RIGHTS

Australians' rights to access internet content and freely engage in online discussions are based less in law than in the shared understanding of a fair and free society. Legal protection for free speech is limited to the constitutionally implied freedom of political communication, which only extends to the limited context of political discourse during an election.[35] The full range of human rights in Australia, unlike in other developed democratic nations, are not protected by a bill of rights or similar legislative instrument, though the country is a signatory to the International Covenant on Civil and Political Rights. Nonetheless, Australians benefit greatly from a culture of freedom of expression and freedom of information, further protected by an independent judiciary. However, the Australian press has consistently expressed concerns about a "culture of secrecy" that

[31] *Jones v. Toben* [2002] FCA 1150 (17 September 2002), http://www.austlii.edu.au/au/cases/cth/FCA/2002/1150.html, accessed June 2010.

[32] Re Lim, "Cronulla Riot: Confiscation of Mobile Phones, Invasion of Privacy and the Curbing of Free Speech," Act Now, March 15, 2006, http://www.actnow.com.au/Opinion/Cronulla_riot.aspx, accessed June 2010;
Les Kennedy, "Man in Court Over Cronulla Revenge SMS," *Sydney Morning Herald*, December 6, 2006, http://www.smh.com.au/news/national/man-in-court-over-cronulla-revenge-sms/2006/12/06/1165081008241.html.

[33] Digital media, for example, is readily used for political campaigning and political protest in Australia. *See* Terry Flew, "Not Yet the Internet Election: Online Media, Political Content and the 2007 Australian Federal Election" (2008) http://eprints.qut.edu.au/39366/1/c39366.pdf.

[34] Global Voices, "Australian Wildfire and Web Tools," February 9, 2009, http://globalvoicesonline.org/2009/02/09/australian-wildfires-and-web-tools/.

[35] Alana Maurushat, Renee Watt, "Australia's Internet Filtering Proposal in the International Context";
Australian Press Council, "Press Law in Australia," http://www.presscouncil.org.au/pcsite/fop/auspres.html#insult, accessed June 2010.

continues to inhibit reporting.[36] A 2007 report commissioned by Australia's Right to Know (ARTK), a coalition of media companies formed to examine free press issues, found that there were over 500 pieces of legislation containing "secrecy" provisions to restrict media publications. It also found barriers to accessing court information, little protection for whistleblowers, and inadequate shield laws to protect journalists.[37]

The Anti-Terrorism Act 2005 revived laws against sedition and unlawful association. The unlawful association provisions have been used widely since their enactment with the banning of several organizations perceived to be potentially dangerous in terms of intentions to commit violent acts.[38] The sedition provisions, however, have not been used. Further, insults against government institutions or officials would not fall within the sedition provisions.[39]

Australian defamation law has been interpreted liberally,[40] and is governed by legislation passed by the states as well as common-law principles. Civil actions over defamation are common and form the main impetus for self-censorship,[41] though a number of cases have established a constitutional defense when the publication of defamatory material involves political discussion.[42] In the online context, the lack of clarity on the responsibility of website operators to delete defamatory comments posted by other users has caused controversy. Court costs and stress associated with defending against suits under defamation laws have caused organizations to leave the country and blogs to shut down.[43] In one prominent case, the operator of the Australian discussion board ZGeek was named as a defendant in a defamation suit over comments posted on the forum that were critical of Greg Smith's conspiracy theory films.[44] Smith sued ZGeek in 2009 for over A$42 million (US$41 million) claiming that he did not land a lucrative film contract due to the comments. Although the Australian courts struck down the defamation suit, ZGeek announced plans to move its discussion forum to another jurisdiction.[45]

---

[36] David Rolph, Matt Vitins, and Judith Bannister, *Media Law: Cases, Materials and Commentaries* (South Melbourne: Oxford University Press, 2010), 44.

[37] Irene Moss, *Report of the Independent Audit into the State of Free Speech in Australia* (Surry Hills, New South Wales: Australia's Right to Know Coalition, 2007), http://www.smh.com.au/pdf/foIreport5.pdf.

[38] Andrew Lynch and George Williams, *What Price Security?* (UNSW Press, 2006) pages 41 to 59.

[39] See note above.

[40] Chris Nash, "Freedom of the Press in Australia," Democratic Audit of Australia, November 19, 2003, http://democratic.audit.anu.edu.au/papers/20031119_nash_press_freed.pdf. For more information generally on press freedom in Australia, see Reporters Without Borders, http://en.rsf.org/australie.html, accessed June 2010.

[41] Irene Moss, *Report of the Independent Audit*; Electronic Frontiers Australia, http://www.efa.org.au/category/defamation/, accessed June 2010.

[42] Human Rights Constitutional Rights, "Australian Defamation Law," http://www.hrcr.org/safrica/expression/defamation.html, accessed June 2010.

[43] See note 32 above; High Court of Australia, "Dow Jones & Company Inc v Joseph Gutnick," news release, December 10, 2002, http://www.hcourt.gov.au/media/dowjones.pdf.

[44] Asher Moses, "Online Forum Trolls Cost me Millions: Filmmaker" The Sydney Morning Herald, July 9, 2009, http://www.smh.com.au/technology/technology-news/online-forum-trolls-cost-me-millions-filmmaker-20090715-dl4t.html.

[45] EFA, "ZGeek Law Suit Struck Down" July 2009, http://www.efa.org.au/2009/07/15/zgeek-defamation-lawsuit-struck-out/.

Criminal defamation charges have also been filed over online content. Adelaide teenager Christopher Cross was convicted in November 2009 of criminal defamation for creating a Facebook group dedicated to criticizing a local police officer. Offensive comments, and some statements encouraging acts of violence against the constable, were posted on the page. Cross was convicted and placed on a two-year and A$500 (US$492) good behaviour bond. If Cross breaches the bond he could conceivably face up to three years in jail.[46] Under Australian law, a person may also bring a defamation case based on information posted by someone outside of Australia providing that the material is accessed in Australia and that the defamed person enjoyed a reputation in Australia.

Law enforcement agencies may search and seize computers, and compel an ISP to intercept and store data from those suspected of committing a crime. Such actions require a lawful warrant. The collection and monitoring of the content of a communication falls within the purview of the Telecommunications (Interception and Access) Act 1979 (TIAA). Call-charge records, however, are regulated by the Telecommunications Act 1997 (TA).[47] It is prohibited for ISPs and similar entities, acting on their own, to monitor and disclose the content of communications without the customer's consent.[48] Unlawful collection and disclosure of the content of a communication can draw both civil and criminal sanctions.[49] The TIAA and TA expressly authorize a range of disclosures, including to specified law enforcement and tax agencies, all of which require a warrant.

ISPs are currently able to monitor their networks without a warrant for "network protection duties," such as curtailing malicious software and spam.[50] Australia has announced plans to accede to the Convention on Cybercrime.[51] Unlike many other countries that have already ratified the convention, Australia is expected to go beyond the treaty's terms in calling for greater monitoring of all internet communications by ISPs. Under the convention, an ISP is only required to monitor, intercept, and retain data when presented with a warrant, and only in conjunction with an active and ongoing criminal investigation. A document leaked in June 2010 from the Attorney General's Department describes a range of possible policy options under which Australian ISPs would be required to monitor, collect, and store information pertaining to all users' communications. This would be done without a warrant and enforced against all users regardless of whether there

[46] Nigel Hunt, "Teen Guilty of Facebook Slur," *Sunday Mail* (SA), November 22, 2009, http://www.adelaidenow.com.au/news/south-australia/teen-guilty-of-facebook-slur/story-e6frea83-1225801651074.
[47] Telecommunications Act 1997, Part 13, http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/.
[48] Part 2-1, section 7, of the Telecommunications (Interception and Access) Act 1979 (TIAA) prohibits disclosure of an interception or communications, and Part 3-1, section 108, of the TIAA prohibits access to stored communications. See http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/.
[49] Criminal offenses are outlined in Part 2-9 of the TIAA, while civil remedies are outlined in Part 2-10.
[50] Alana Maurushat, "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Obfuscation Crime Tools?" *University of New South Wales Law Journal* 16, no. 1, forthcoming.
[51] Convention on Cybercrime, Council of Europe, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG, accessed June 2010.

is a criminal investigation.[52] This compulsory data-retention policy, if enacted, could become a great threat to online freedom in Australia. The document is not official policy in Australia nor has it evolved into a concrete proposal or bill. As of December 2010, therefore, it was unclear whether such a policy would be realized in Australia.

Users do not need to register to use the internet, nor are there restrictions placed on anonymous communications. However, under a new election law in the state of South Australia that came into effect in January 2010, any individual posting a political comment in the run-up to local elections would be required to do so with their real name and address. The law applied to blogs and online news sites and non-compliance would draw a fine of up to A$1,250 (US$1,230). Following a public outcry, the state's attorney general and premier agreed to repeal the law.[53] Regarding mobile-phone users, verified identification information is required to purchase any prepaid mobile service. Additional personal information is required for the service provider before a phone may be activated. All purchase information is stored while the service remains activated, and it may be accessed by law enforcement and emergency agencies providing there is a valid warrant.[54]

Users of social-networking sites and similar applications have been threatened with physical violence and extralegal intimidation by other users, though not by state authorities. For example, a number of pages were established to memorialize Trinity Bates, a young girl who was abducted and brutally murdered in February 2010, and to call for violence against the accused killer. These sites were defaced by anonymous users who uploaded child pornography, and online and offline threats were then made against the suspected vandals.[55]

There have been a number of politically motivated cyberattacks, more specifically known as denial-of-service attacks (DoS) which have led to websites being inaccessible or flooded with substituted content for various lengths of time. The most well known attack is commonly referred to as Operation Titstorm. In February 2010, an internet group of activists known as Anonymous launched a DoS attack against the Australian Parliament House website in protest of the proposed internet filter.[56] The attack brought down Parliament's website for three days by bombarding it with pornographic images. It is unknown whether the Australian authorities have taken any measures to address politically

[52] Asher Moses, "Web Snooping Policy Shrouded in Secrecy," *The Age*, June 17, 2010, http://www.theage.com.au/technology/technology-news/web-snooping-policy-shrouded-in-secrecy-20100617-yi1u.html.
[53] Nate Anderson, "Internet Uprising Overturns Australian Censorship Law," Ars Technica, February 2, 2010, http://arstechnica.com/tech-policy/news/2010/02/internet-uprising-overturns-australian-censorship-law.ars; "South Australian Government Gags Internet Debate," News.com.au, February 2, 2010, http://www.news.com.au/technology/south-australian-state-government-gags-internet-debate/story-e6frfro0-1225825750956.
[54] ACMA, "Pre-paid Mobile Services—Consumer Information Provision Fact Sheet," http://www.acma.gov.au/WEB/STANDARD/pc=PC_9079, accessed June 2010.
[55] Emily Bourke and Kerrin Binnie, "Trinity Murder Inflames Facebook Debate," Australian Broadcasting Corporation (ABC), February 25, 2010, http://www.abc.net.au/news/stories/2010/02/25/2829635.htm.
[56] David Kravets, "Anonymous Unfurls 'Operation Titstorm'," *Wired Magazine*, February 10, 2010, http://www.wired.com/threatlevel/2010/02/anonymous-unfurls-operation-titstorm/#.

motivated DoS attacks.[57] More severe cyber attacks such as on the nation's critical infrastructure (such as electric grids, hospitals, banks) have occurred as well, though, to date, these have mostly been attacks on banking infrastructure for financial motives.[58]

[57] Websites typically cannot take preventative measures to ensure that they are not subject to a denial of service attack. Measures may only be taken once an attack has commenced to mitigate against damages.
[58] AusCERT Conference (2009), closed session invite only workshop on cybercrime, Chatham House Rules.

AZERBAIJAN

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Partly Free**
Obstacles to Access	n/a	15
Limits on Content	n/a	15
Violations of User Rights	n/a	18
Total	**n/a**	**48**

POPULATION: 9.1 million
INTERNET PENETRATION 2009: 27 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

As Azerbaijan's internet usage has exploded in recent years, the authorities have attempted to exercise greater control over the medium, though it remains much less restricted than print and broadcast media, which are the main sources of news for most citizens. In early 2010, the government expressed its intent to require internet-service providers (ISPs) to obtain licenses and sign formal agreements with the Ministry of Communications and Information Technology, although those plans seem to have been put on hold.[1] There have sporadically been blocks imposed on certain websites and some officials have also called for the licensing of websites, including online news outlets. The authorities have used the criminal justice system to limit online expression, and two bloggers were imprisoned in 2009; the pair was released in November 2010 following an international campaign on their behalf.

The first e-mail message in Azerbaijan was sent in 1991 at the Institute of Information Technologies (Azerbaijan National Academy of Sciences), and the first internet connections were established in 1994. However, open access for all citizens was made available only in 1996. The government began implementing policies aimed at lowering prices in 2007, and the internet is now somewhat more accessible for businesses and certain segments of the population.[2] However, despite the notable increase in internet penetration, quality remains

[1] "Lisenziya: Çixiş Yolu, Ya Təhlükə?" Media Forum, April 16, 2010, http://www.mediaforum.az/articles.php?article_id=20100416110158693&lang=az&page=04.

[2] "Beynəlxalq Telekommunikasiya İttifaqı: Azərbaycan mobil rabitə tariflərinin azaldılması üzrə lider-ölkədir" APA, February 24, 2010, http://az.apa.az/news.php?id=178885.

low, as most people still use slow dial-up connections. The first license for third-generation (3G) mobile telephony was issued in mid-2009 to Vodafone-Azerfon, but prices for high-speed mobile internet are still very high.

OBSTACLES TO ACCESS

According to the International Telecommunication Union, 27 percent of the population had access to the internet in 2010, a significant increase from 2008, when the penetration rate was roughly 14 percent.[3] However, only 12 percent of Azerbaijanis own a computer. Many people use computers at work, school, or internet cafes, which are particularly popular in smaller towns and less affluent areas.

High cost remains a key obstacle to access, although other factors—such as education, lack of computer literacy, socioeconomic status, and gender—also play a role. Average monthly prices range from 20 to 50 Azerbaijani manats (US$25 to US$62) for unlimited access at 1 Mbps speed via ADSL broadband technology.[4] While these prices are significantly lower than several years ago, they are still out of reach for many Azerbaijanis; the average monthly salary is estimated to be 304 manats (US$378).[5] Consequently, only 5.9 percent of the population have fixed internet subscriptions, and just over 1.1 percent subscribe to broadband access.[6] Moreover, ADSL users typically must pay for their own modems, which start at US$25. According to official statistics, 90 percent of internet subscribers use dial-up connections with speeds of no more than 56 Kbps, particularly those living outside of Baku.[7] Among different demographic groups, young, urban men are most likely to have access to the internet.

Access to advanced web applications like the social-networking site Facebook and the microblogging service Twitter is not restricted. In fact, social-networking sites are routinely used to disseminate content that is critical of the government. The number of registered Facebook users has grown from approximately 105,000 at the beginning of 2010 to over 279,000 as of the end of December.[8] Because most users access the internet at painfully slow dial-up speeds, they have significant difficulties accessing material on some websites, especially photos, audio and video recordings, and streaming audiovisual content.

[3] International Telecommunication Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx, accessed February 16, 2011.
[4] "Internet Prices in Azerbaijan Equal to Other Countries of Region," ABC.az, April 14, 2010, http://abc.az/eng/news_14_04_2010_44154.html.
[5] Nijat Mustafayev, "Average Salary Rises 4% in Azerbaijan During January–March," Azeri-Press Agency (APA), April 20, 2010, http://en.apa.az/news.php?id=120385.
[6] International Telecommunication Union, "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#, accessed August 1, 2010.
[7] "Azərbaycanda 3,7 milyon internet istifadəçisi var? Azadliq, July 4, 2010, http://azadliq.info/cemiyyet/1982.html.
[8] Facebakers, "Facebook Statistics Azerbaijan," http://www.facebakers.com/countries-with-facebook/AZ/, accessed January 1, 2011

Delta Telecom is the main ISP and serves as the backbone for the country's 30 retail-level ISPs, but the company's ownership structure is not transparent. The largest ISP operating outside of Baku is the state-owned Aztelecom. Another company, Azertelecom, is currently working to create its own fiber-optic network, and in the future it could be a major competitor for Delta Telecom's business.

Usage of mobile phones in Azerbaijan has been growing steadily. In 2009, there were nearly 88 mobile subscriptions per 100 inhabitants.[9] There are three mobile-service providers using the globally dominant GSM standard: Azercell, Azerfon, and Bakcell. Another company, Catel, uses the alternative CDMA standard. In 2009, Azerfon, in a partnership with Britain's Vodafone, became the only company to obtain a license for 3G service. The use of the internet through mobile phones has so far been limited, due in part to the high cost of subscriptions.

Azerbaijan does not have an independent regulatory body for the telecommunications sector. Currently, the basic regulatory functions are performed by the Ministry of Communications and Information Technology pursuant to the 2005 Law on Telecommunications. Internet domain names in Azerbaijan cannot be obtained online and require an in-person application, subjecting the process to bureaucratic red tape and possible corruption.

LIMITS ON CONTENT

The Azerbaijani government does not engage in widespread censorship of the internet. However, domestic observers reported that on several occasions during 2009, the government temporarily blocked public access to websites that were popular for lampooning the president. There were reportedly greater restrictions on the internet in the autonomous exclave of Nakhchivan, where residents claimed they were unable to view the websites of the opposition newspapers *Azadliq* and *Bizim Yol*. Access has also been denied to the website of Radio Free Europe/Radio Liberty's Azerbaijani service, www.azadliq.org. Each episode of blocking lasted only a few days. In 2009, just before municipal elections, authorities also blocked public access to two websites of an independent nongovernmental organization (NGO), the Election Monitoring Center, although the sites remained accessible from abroad. Since the government does not officially admit to blocking websites, there is no established process through which affected entities can appeal.

There has been an incredible growth in blogging since 2007. Thanks to the introduction of Azerbaijani-language blogging platforms, a new generation of bloggers has appeared and started writing on issues that have never been covered by traditional media.

[9] International Telecommunication Union, "ICT Statistics 2009—Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#, accessed August 1, 2010.

There are about 27,000 blogs in Azerbaijan, most of which are written in the Azerbaijani language. Only 1,000 blogs are written in English, Russian, and other languages. Many bloggers, such as Ali Novruzov, Arzu Geybulla, and Ilgar Mammadov, are well known for their independent views.

Youth are the most active bloggers in Azerbaijan, and have encountered the first censorship efforts associated with blogging. Two activists from the OL! and AN youth movements, Emin Milli and Adnan Hajizade, were arrested in 2009. They were convicted on dubious charges of hooliganism, having been attacked by two men at a restaurant in what was apparently a government-organized provocation, but the real reason for their arrest is thought to be their posting of a satirical piece on the video-sharing site YouTube. The video mocked the government's reported decision to import donkeys at exorbitant prices, suggesting that donkeys are treated better than ordinary people in Azerbaijan.[10] Internet campaigns calling for the two men's release were blocked several times by the authorities. The pair was released in November 2010 following international and domestic pressure for their release,[11] but they remain prohibited from leaving the country. While traditional media journalists practice extensive self-censorship, expression in the online sphere has been freer, though the two bloggers' arrest had a chilling effect on other internet users.

Youth activists, organizations, and movements are widely represented in social media. They provide information, organize activities and events, and arrange flash mobs via the internet. Opposition parties, traditional NGOs, and state organizations started to use these tools in advance of the November 2010 elections, but their efforts are still very weak. Although many Baku-based candidates used the internet for campaigning, the use of such methods in other regions was seen as less effective.

VIOLATIONS OF USER RIGHTS

Article 47 of the constitution guarantees freedom of thought and speech.[12] In addition, Article 50 stipulates that everyone has the right to distribute information, that freedom of the mass media is guaranteed, and that censorship is prohibited. In practice, however, the authorities aggressively use various forms of legislation to stifle freedom in the print and broadcast media. Libel is a criminal offense and traditional media journalists who criticize the authorities are frequently prosecuted and imprisoned. The judiciary is largely

[10] The video is available at http://www.youtube.com/watch?v=Aaecvg7xCIk.

[11] Reporters without Borders, "Interview with the newly-released video blogger and netizen Adnan Hajizade," November 30, 2010, http://en.rsf.org/azerbaijan-interview-with-the-newly-released-30-11-2010,38922.html; Freedom House, "Release of Bloggers a Positive Step for Freedom of Expression in Azerbaijan," November 19, 2010, http://www.freedomhouse.org/template.cfm?page=70&release=1280

[12] The constitution is available in English at http://www.president.az/azerbaijan/constitution/?locale=en.

subservient to the executive branch.[13] Under the Law on Mass Media of 1999, the internet is designated as part of the mass media. Therefore, all rules applied to traditional media, which press freedom advocates consider problematic, could be used for internet regulation as well.[14] To date, however, the only known case of prosecution for online expression has been the above mentioned two bloggers, charged under laws related to hooliganism. In November 2010, it was announced that the government-controlled Press Council will start monitoring online news sources for their compliance with the rules of professional journalism.[15]

It is unclear to what extent security bodies track user data in Azerbaijan. However, some state universities warn students that they will encounter problems if they participate in online political activism. Students are instead urged to be very active in defending the government and its positions in their posts and comments on Facebook and other social media. It is widely believed that the internet communications of certain individuals are monitored, especially foreigners, known activists, and business figures. Moreover, most users do not have licenses for the software on their computers, which leaves them vulnerable to security threats like viruses and other malicious programs that could be used to monitor their activity, among other functions. According to some estimates, pirated programs account for 80 percent of the software market in the country.

In one recent case, student Parviz Azimov was expelled from Lankaran State University early 2009 after writing a blog post on corruption during exams, which was later republished by one local and two national newspapers. Protests near the Ministry of Education in Baku by the Dalgha youth movement, to which Azimov belonged, combined with pressure from international organizations, led to a court decision allowing him to return to the university.

Ali Abbasov, the minister of communications and information technology, called in April 2010 for a licensing system that would apply to news websites. He claimed that such a system would help eliminate unspecified "illegal activities," noting that "there is no mechanism today to influence" such sites. The head of the country's National Television and Radio Council made similar comments later that month, proposing stronger controls on internet radio and television outlets,[16] although in July, another government official said that the government did not have any immediate plans to introduce such measures.

[13] Karin Karlekar, ed., "Azerbaijan," *Freedom of the Press 2010* (New York, Freedom House 2010) http://www.freedomhouse.org/template.cfm?page=251&year=2010

[14] "Law of the Republic of Azerbaijan "About Mass Media,""Azerbaijan National Academy of Sciences, http://ict.az/en/index.php?option=com_content&task=view&id=477&Itemid=95.

[15] "Control Over Online Sources and Facebook-like sites in Azerbaijan," Today.az, November 27, 2010, http://www.today.az/view.php?id=77287.

[16] Mina Muradova, "Azerbaijani Government Pondering Ways to Control the Web," Eurasianet.org, May 13, 2010, http://www.eurasianet.org/node/61060.

Wrongful access to a computer, for instance through viruses and security breaches, is punishable under Chapter 30 of the criminal code.[17] Internet security is also dealt with in the Law on National Security of 2004 and the Law on Protection of Unauthorized Information of 2004. Hacking attacks aimed at the Azerbaijani internet often come from Armenian internet protocol (IP) addresses. The timing of such attacks typically coincides with politically sensitive dates related to the unresolved territorial conflict between the two countries. Sometimes attacks occur after high-profile political statements. The apparently Armenian-based attacks have targeted the websites of entities like the Ministry of Communications and Information Technology, the National Library, and the public television broadcaster. It is very rare for local hackers to attack Azerbaijani websites. The Anti-Cybercriminal Organization is the main body working against cyber attacks in Azerbaijan. The country ratified the Council of Europe's Convention on Cybercrime in March 2010, and it took effect in July.

[17] An unofficial English translation of the criminal code is available at http://www.legislationline.org/download/action/download/id/1658/file/4b3ff87c005675cfd74058077132.htm/preview.

BAHRAIN

	2009	2011
INTERNET FREEDOM STATUS	n/a	Not Free
Obstacles to Access	n/a	11
Limits on Content	n/a	22
Violations of User Rights	n/a	29
Total	n/a	62

POPULATION: 1.3 million
INTERNET PENETRATION: 54 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Bahrain has one of the highest internet penetration rates in the Middle East, but as more people have gained access to new technologies, the government has increasingly attempted to curtail their use for disseminating and obtaining politically sensitive information. Bahrain has been connected to the internet since 1995. In 1997, an internet user was arrested for the first time, for sending information to an opposition group outside the country.[1] In 2002, the Ministry of Information (MOI) made its first official attempt to block websites containing content that was critical of the government. Today, over 1,000 websites are blocked in Bahrain.[2]

Censorship of online media is implemented under the 2002 press law. The restrictions have been extended to mobile telephones, and the use of Blackberry services to disseminate news is banned. The government intensified its crackdown on internet activists and online publications in the period leading to the October 2010 elections by arresting two bloggers and shutting down several websites and online forums critical of the state authorities. [3]

[1] Initiative For an Open Arab Internet, "Implacable Adversaries: Arab Governments and the Internet: Bahrain," December 2006, http://old.openarab.net/en/node/350.
[2] Reporters Without Borders, "Countries Under Surveillance: Bahrain," http://en.rsf.org/surveillance-bahrein,36665.html, accessed August 17, 2010.
[3] Bahrain Center for Human Rights, "New Web Crackdown Blocks Dozens of Websites and Electronic Forums in Bahrain," September 4, 2010, http://bahrainrights.hopto.org/en/node/3287.

OBSTACLES TO ACCESS

According to some measures, Bahrain is the second most connected country in the Arab world,[4] and the number of internet users has risen rapidly, from 40,000 in 2000 to 649,300 in 2009.[5] In mid-2009, there were approximately 139,000 internet subscriptions, of which 53.9 percent were ADSL, 30.7 percent were wireless, 12.6 percent were mobile broadband, and 2.8 percent were dial-up.[6] Internet access is widely available at schools, universities, and coffee shops, where Bahrainis often gather for work and study. However, when it comes to the quality of services, a report issued in 2009 suggests that Bahrain's broadband connections cannot adequately support modern internet applications, such as video and file sharing.[7]

While price competitiveness is increasing, subscription prices are still relatively high considering the restricted speeds and download limits. This is due to the fact that most internet-service providers (ISPs) are dependent on leased access to the network of Batelco, the dominant, partly state-owned telecommunications firm.[8]

Bahrain has one of the highest mobile-phone penetration rates in the region, with 118 mobile subscriptions per 100 inhabitants.[9] Some of the latest generations of mobile phones, such as Apple's iPhone, are available in the country, but they are still very expensive. Although the use of Blackberry phones is on the rise, particularly among the business community, the authorities in April 2010 banned Blackberry users from sending news bulletins through text messages and threatened the individuals and newspapers responsible for the messages with legal action.[10]

The government routinely prohibits the publication of advanced Web 2.0 content and blocks interactive exchange, particularly when they do not support its political agenda. Access to the video-sharing site YouTube, social-networking site Facebook, and the

[4] This ranking includes internet access as well as fixed and mobile telephone lines. Mohamed Marwen Meddah, "Total Country Connectivity Measure for the Arab World," Startup Arabia, August 20, 2009, http://www.startuparabia.com/2009/08/total-country-connectivity-measure-for-the-arab-world.

[5] International Telecommunication Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx, accessed February 16, 2011.

[6] Telecommunications Regulatory Authority (TRA), *Telecommunications Market Indicators in the Kingdom of Bahrain* (Manama: TRA, March 2010), slides 20 and 23, http://www.tra.org.bh/en/pdf/TelecommunicationsmarketsindicatorsintheKingdomofBahrain.pdf.

[7] Said Business School (University of Oxford) and Universidad de Oviedo, *Broadband Quality Score: A Global Study of Broadband Quality* (Oxford: Said Business School; Oviedo: Universidad de Oviedo, September 2009), http://www.sbs.ox.ac.uk/newsandevents/Documents/Broadband%20Quality%20Study%202009%20Press%20Presentation%20(final).pdf.

[8] Daniel Munden, "Gateway to Success," *Gulf Daily News*, August 26, 2009, http://www.gulf-daily-news.com/NewsDetails.aspx?storyid=258311.

[9] TRA, *Telecommunications Market Indicators in the Kingdom of Bahrain*, slide 10.

[10] Bahrain Center for Human Rights, "Authorities Ban Blackberry Users from Sending News Bulletins," IFEX, April 15, 2010, http://ifex.org/bahrain/2010/04/15/blackberry_ban/.

microblogging site Twitter is available, although individual pages on each of those platforms are often blocked (see "Limits on Content"). The Arabic regional portal and blog-hosting service Al-Bawaba has been blocked since 2006, and the Bahraini blog aggregator Bahrainblogs.org, which served as a means for Bahraini bloggers to interconnect, was blocked in 2009. In 2010, the Information Affairs Authority (IAA), a new government agency that replaced the MOI earlier in the year, banned the use of video and audio reports on the website of the *Al-Wasat* newspaper, seemingly after the outlet webcast several audio programs critical of the authorities. Moreover, the IAA blocked the website of the largest political society Al-Wefaq reportedly after the group announced plans to start an audio and video service through the site.[11]

There are 12 ISPs serving Bahraini users, but the major providers are Batelco, MENA Telecom, Zain, and the recently launched VIVA. Most ISPs lease network access from Batelco, although the firm was fined in late 2009 for refusing to grant MENA Telecom direct access to an international cable.[12] According to Bahrain's Telecommunications Regulatory Authority (TRA), some 31 ISP licenses have been granted, but only 12 providers are in business.[13] There have been no reported instances of ISPs being denied registration permits. Three of the major ISPs are also the only mobile operators in Bahrain: Batelco, Zain, and VIVA.

Mobile-phone services and ISPs are regulated by the TRA under the 2002 Telecommunications Law. Although the TRA is an independent organization on paper, its members are appointed by the government, and its chairman reports to the minister of state for cabinet affairs with responsibility for telecommunications, Sheikh Ahmed bin Attiyatallah al-Khalifa (a member of the ruling family). The TRA has issued several regulations that were not welcomed by consumers, including measures that could potentially violate individual privacy rights.[14]

LIMITS ON CONTENT

Online media in Bahrain are governed by the Press and Publications Law of 2002, which stipulates prison sentences of up to five years for publishing material that is offensive to

[11] Bahrain Center for Human Rights, "Crackdown Against Civil Rights and Free Expression Results in the Blockage of the Website of the Largest Political Society," September 18, 2010, http://www.bahrainrights.org/en/node/3366.
[12] "TRA Fines Batelco $13m on Access Curbs," Trade Arabia News Service, November 25, 2009, http://www.tradearabia.com/news/it_170919.html.
[13] TRA, "Market Information: Number of Licenses Issued," http://www.tra.org.bh/en/marketstatistics.asp, accessed August 17, 2010.
[14] Geoffrey Bew, "'Big Brother' Move Rapped," *Gulf Daily News*, March 25, 2009, http://www.gulf-daily-news.com/ArchiveNewsDetails.aspx?date=03/25/2009&storyid=246587.

Islam or the king, or that is perceived as undermining state security or the monarchy.[15] According to some estimates, the IAA (formerly the MOI) has blocked and shut down more than 1,000 websites, with a focus on sites that are critical of the Bahraini government, parliament, and ruling family, and including human rights websites, blogs, and online forums.[16] The IAA can order the blocking of a website without referring the case to a court. It has instructed all ISPs to "prohibit any means that allow access to sites blocked by the ministry."[17]

On January 14, 2009, the MOI issued a ministerial order requiring all ISPs to block websites containing pornography or material that may provoke violence or religious hatred.[18] It also threatened to revoke the license of any operator violating the decree. The ISPs have consequently begun using a commercial filtering system and posting an explicit block page with a reference to the ministerial order.[19] The filtering is based on keyword density, the manual entry of URLs, and certain website categories, including potential circumvention tools like Google page translate and Google cached pages.

Website administrators face the same libel laws that apply to print journalists, and they are held jointly responsible for all content posted on their sites or chat rooms. In 2009 the website of the Democratic National Work Society was blocked for the second time after it published an article about the so-called Al-Bandar report, which described an alleged anti-Shiite conspiracy within the Sunni-led government. The authorities required the removal of the article as a condition for lifting the block, but the society rejected the demand and the case went to court.[20] In February 2009, the MOI said it had lifted blocks on multiple websites after they removed the banned content.[21] Many webmasters have added rules to their online forums that prohibit posts criticizing the ruling family, and they have begun banning users who attempt to post such comments to avoid having their sites blocked.

In practice, many websites run by national or international nongovernmental organizations (NGOs) are inaccessible. For example, the websites of the Arab Network for Human Rights Information (ANHRI) and the Bahrain Center for Human Rights (BCHR) have been blocked. The MOI has also issued orders to ban material about certain cases that could implicate members of the royal family, such as the alleged anti-Shiite conspiracy and a

[15] Press and Publications Law of 2002 of the Kingdom of Bahrain (No.47 of 2002). A copy can be found at: http://mahmood.tv/bahrain/bahrain-politics-2/bahrain-politics/press-law-472002-arabic/.
[16] Reporters Without Borders, "Countries Under Surveillance: Bahrain."
[17] Reporters Without Borders, "Authorities Step Up Offensive Against Journalists and Websites," news release, May 14, 2009, http://en.rsf.org/spip.php?page=article&id_article=33042.
[18] Frederik Richter, "Bahrain Web Crackdown Triggers Calls for Reform," Reuters, February 9, 2009, http://www.reuters.com/article/idUSTRE5183Y320090209.
[19] OpenNet Initiative, "Country Profile: Bahrain," August 06, 2009, http://opennet.net/research/profiles/bahrain#footnote34_6d3d5g9.
[20] Ibid.
[21] "Information Ministry Reopens Blocked Websites," [in Arabic[*Alwasat*, February 13, 2009, http://www.alwasatnews.com/2352/news/read/37295/1.html.

case involving alleged corruption by a government minister.[22] Even Google Earth was briefly rendered inaccessible so that Bahraini citizens could not examine the estates of the royal family;[23] it was unblocked after concerted public and media pressure. Blocking decisions and policies are not transparent, and users do not always get a block message, especially when they try to access banned political websites. For some blocked sites, DNS tampering is used, and users simply receive error messages such as "The page cannot be displayed."[24] Webmasters do not receive notifications that their sites have been banned.

Apart from websites, the government routinely blocks blogs and individual pages on social-networking sites such as Facebook, Twitter, and YouTube. For example, several Bahraini blogs were blocked in 2009, including those maintained by human rights activists Abduljalil Alsingace (Alsingace.katib.org) and women's rights activist Ghada Jamsheer (Bahrain-eve.blogspot.com). In January 2010, authorities blocked access to a Twitter page called "Free Bahrain." It was operated by a Bahrain resident who posted links and news on the human rights situation in the country.[25] The same woman's personal channel on the YouTube video-sharing site, which mostly contained critical footage, was also blocked.[26] Moreover, in June 2010, the authorities blocked a popular blog called Sanawat al-Jareesh, which provided an unofficial account of Bahrain's history.[27] And most recently, amidst the crackdown in advance of the November election, the personal website and the Facebook page of an opposition activist Abdul Wahb Hussain were also blocked.

Although technically the law does allow affected individuals to appeal a block within 15 days, no such case has yet been adjudicated even several years after the blocking action in question. For example, a legal challenge mounted by the Waad political group has languished in the courts, and the blocking order against its website remains in place. The website is now accessible due to pressure exerted on the authorities, but the block could be reinstated arbitrarily.[28]

Since the enactment of the 2002 Telecommunications Law, which assigns penalties for illicit use of the internet, users have adopted a culture of self-censorship. Bahraini bloggers, numbering close to 200, usually prefer to remain anonymous, and security personnel do not hesitate to pursue or harass "irritating" journalists and bloggers.[29] Users

[22] Bahrain Center for Human Rights, "Authorities Reinforce Sweeping Media Ban, Internet Censorship on Controversial Report," news release, November 28, 2007, http://bahrainrights.hopto.org/en/node/1635;
Bahrain Center for Human Rights, "Dealing in Double Standards Whilst Fighting Corruption, and Violating Freedom of Opinion and Expression," news release, April 18, 2010, http://bahrainrights.hopto.org/en/node/3075.
[23] Reporters Without Borders, "Countries Under Surveillance: Bahrain."
[24] OpenNet Initiative, "Country Profile: Bahrain."
[25] Bahrain Center for Human Rights, "Authorities Block Human Rights Page on Twitter Website," news release, January 20, 2010, http://bahrainrights.hopto.org/en/node/3023.
[26] "Minister Blocks YouTube Channel," IFEX, January 22, 2010, http://www.ifex.org/bahrain/2010/01/22/youtube_channel_blocked/.
[27] "Information Ministry blocks Sanawat Al-Jareesh," [In Arabic] *Al-Bilad,,* June 11 2010, http://www.albiladpress.com/news_inner.php?nid=79281&cat=1.
[28] More information can be found on the *Alwasat*, website, http://www.alwasatnews.com/2609/news/read/326019/1.html.
[29] Reporters Without Borders, "Countries Under Surveillance: Bahrain."

tend to avoid certain subjects, including criticism of the ruling family and government practices; the Al-Bandar report, which is referred to as the "xx-report," and human rights issues.

Bahrain's online community is small but dynamic. As of January 2008, there were over 535 websites based in Bahrain. In addition to the 200 blogs, they included 111 public forums and several dozen governmental sites.[30] The use of proxy services, dynamic internet protocol (IP) addresses, and virtual private network (VPN) applications allow the majority of users in Bahrain to access blocked websites, although many less savvy users are not as successful. In fact, the government regularly blocks access to proxy sites and tools that enable circumvention of online filters and censors, including applications that allow browsing of other websites, such as Google page translation, Google cached pages, and online mobile emulators, requiring users to be consistently creative and adapt.

Bahrainis use the internet to debate sensitive issues and to exchange content that is not available in the traditional media. The most popular platform is the banned Bahrainonline.org—the largest independent news forum with over 50,000 members—where coverage of regular street protests is posted along with oppositionist articles. Multiple independent online news sites have emerged in the last few years, but many have had to close due to constant harassment by the authorities. For example, the sites Alsaheefa.net and Awaal.net were closed after three journalists were charged with inciting hatred of the government, insulting the regime, and fostering sectarianism in 2008.[31] Tools like Twitter, the social-networking site Facebook, YouTube, and mobile-phone text messages have been well utilized by Bahraini individuals and human rights organizations such as the Bahrain Center for Human Rights to organize protests and promote civil rights.[32] These tools have started to play even more significant role following the pre-election crackdown in 2010; after many forums and critical websites were blocked, many Bahrainis turned to Twitter and Facebook to voice their opinions and campaign against the government actions.[33]

[30] Bahrain Center for Human Rights, "Internet Censorship Denies Citizens Access to Popular Public Forums, News, Alternative Information," IFEX, January 3, 2008, http://www.ifex.org/bahrain/2008/01/03/internet_censorship_denies_citizens/.
[31] Bahrain Center for Human Rights, "Three Writers for Banned Internet Site Convicted of Criminal Defamation, Fined," news release, October 23, 2007, http://bahrainrights.hopto.org/en/node/1500; Reporters Without Borders, "Press Law Amendments Hailed, but Journalists Still Face Jail and Websites Risk Closure," news release, July 03, 2008, http://en.rsf.org/bahrain-press-law-amendments-hailed-but-03-07-2008,27741.html.
[32] IFEX, "Case Study: BCHR combats censorship with creativity, using film, photography and e-advocacy", http://www.ifex.org/campaigns/e-advocacy/index7.php, accessed February 15, 2011.
[33] Frederik Richter, "Lively Bahrain social media face government pressure," Reuters, October 21, 2010, http://www.reuters.com/article/idUSTRE69K2OG20101021.

VIOLATIONS OF USER RIGHTS

Although freedom of expression is enshrined in the constitution, the guarantees are qualified by the phrase "under the rules and conditions laid down by law," which essentially negates them.[34] Similarly, the 2002 press law promises free access to information, but "without prejudice to the requirements of national security and defending the homeland." Bahraini journalists have argued that these loosely worded clauses allow for arbitrary interpretation.[35] There is no law that guarantees users' privacy. A proposed cybercrimes law has been under consideration since 2005.[36]

Online journalists and others face prison terms of up to five years for violations of the 2002 Press and Publications Law (see "Limits on Content").[37] In addition, the 2002 Telecommunications Law contains penalties for illicit practices including the transmission of messages that are offensive to public policy or morals.[38] This vague phrase has been used by the government to question and prosecute several bloggers and journalists, including moderators of Bahrainonline.org who were arrested after a UN report on human rights in Bahrain was published on their forums; they were released due to public pressure, but their case has remained open since 2005 and they can be taken back to court at any time.[39]

Users can be prosecuted for libeling officials, as in the case of Mahmood al-Yousif, who was accused of libeling Bahrain's agriculture minister after he found fault with a statement made by the minister.[40] In May 2009, Hasan Salman was arrested and accused of publishing what authorities claimed were confidential names of employees of the national security apparatus. He was tried under the penal code and sentenced to three years in jail.[41] In April 2010, as previously noted, the authorities threatened to punish individuals and newspapers responsible for sending news bulletins through Blackberry text messages

[34] Constitution of the Kingdom of Bahrain, available at http://www.shura.bh/en/InformationCenter/Pages/Documents.aspx.
[35] "Bahrain," in *Media Sustainability Index 2008* (Washington, DC: IREX, 2009), http://irex.org/programs/MSI_MENA/2008/MSIMENA_bahrain.asp.
[36] "New law to protect from cyber crime is presented to the House of Representatives," [in Arabic] *Alayam*, April 28, 2010, http://www.alayam.com/Articles.aspx?aid=17707.
[37] Committee to Protect Journalists, "Bahrain," in *Attacks on the Press 2009* (New York: Committee to Protect Journalists, February 2010), http://www.cpj.org/2010/02/attacks-on-the-press-2009-bahrain.php.
[38] Telecommunications Law of the Kingdom of Bahrain.
[39] Luke Schleusener, "From Blog to Street: The Bahrain Public Sphere in Transition," *Arab Media and Society* no. 1 (Spring 2007), http://www.arabmediasociety.com/?article=15.
[40] Mahmood Nasser al-Yousif, "Bahraini Blogger: Freedom of Speech Stifled," *Mahmood's Den* (blog), November 26, 2007, http://mahmood.tv/about/in-the-news/bahraini-blogger-freedom-of-speech-stifled/.
[41] "Bahrain: Citizen Sentenced to Three Years in Prison," Free Hasan Salman, September 18, 2009, http://freehasan.no-ip.org/?p=310.

without a government license.[42] One member of parliament is on record as recommending that transgressors be hanged.[43]

Two bloggers were arrested amidst security crackdown against activists and dissidents in the period leading to the 2010 elections. In August 2010, Abduljalil Alsingace—a blogger, academic, and a leading figure in the Haq opposition group—was arrested when returning from London, where he participated in a seminar on the worsening human rights situation in Bahrain. Al-Singace's website, on which he had criticized the systematic use of torture and discrimination against the Shiites, was closed down by the authorities in February 2009. In September 2010, Ali Abdulemam, an online activist and the founder of Bahrainonline.org, was also arrested,[44] this time for allegedly disseminating false information on the forum. During their court hearing in October, both Alsingace and Abdulemam said that they had experienced severe beatings on the head, long standing hours, deprivation of sleep, and threats of rape. They also complained of being denied access to their families and lawyers and being kept in solitary confinement. [45]

In 2007, the MOI ordered the registration of all websites hosted in the country or abroad that featured information about the kingdom. This decision met with significant opposition from a large number of website owners, who tacitly decided not to register their sites. The regime then reversed its position, and registration became optional.[46] The TRA also requires users to obtain licenses to use wireless fidelity (WiFi) and worldwide interoperability for microwave access (WiMax) connections.[47] The government does not allow the sale and use of prepaid mobile-phone chips without registration. In March 2009, the TRA issued a new regulation that would force telecommunications companies to keep records of customers' phone calls, e-mails, and website visits in Bahrain for up to three years; the companies would also be obliged to grant the security services access to the data.[48] Media reports have quoted an official source as saying that some websites are monitored on a daily basis.[49] In the case of Hasan Salman, who was jailed for publishing names of national security employees,[50] his online activities were monitored without a

[42] Bahrain Center for Human Rights, "Authorities Ban Blackberry Users from Sending News Bulletins."
[43] "MP Al-Dossari calls for hanging journalists of the associations' newsletter," [In Arabic] *Manama Voice*, February 23, 2010, http://www.manamavoice.com/index.php?plugin=news&act=news_read&id=2574.
[44] Bahrain Center for Human Rights, "Prominent Bahraini Blogger and Online Activist Under Arrest," September 6, 2010 http://www.bahrainrights.org/en/node/3300.
[45] Bahrain Center for Human Rights, ""Terrorist Network's First Hearing – Trial Testimonies," October 28, 2010 http://www.bahrainrights.org/en/node/3540.
[46] Reporters Without Borders, "Countries Under Surveillance: Bahrain."
[47] Geoffrey Bew, "Technology Bill Rapped," *Gulf Daily News*, July 20, 2006, http://www.gulf-daily-news.com/NewsDetails.aspx?storyid=149891.
[48] Bew, "'Big Brother' Move Rapped."
[49] Bahrain Center for Human Rights, "Several Websites Blocked by Information Ministry on Pretext of Crisis Involving Sectarian Religious Tensions," IFEX, July 2, 2008, http://www.ifex.org/en/content/view/full/95015/.
[50] "Arbitrary Detention of a Citizen for Disseminating Information," Free Hasan Salman, June 21, 2009, http://freehasan.com/?p=107.

judicial order.[51] The country's cybercafes are subject to increasing surveillance. Oversight of their operations is coordinated by a commission consisting of members from four ministries, which ensures strict compliance with rules prohibiting access for minors and requiring full visibility of computer terminals.[52]

Cyberattacks against human rights and other websites are common in Bahrain. It is believed that hackers associated with the government crash sites at sensitive times when there is a need to stop the spread of information. The website Aafaq, which covers human rights and democracy issues in the Arab world, has been hacked by technicians from the Bahrain General Intelligence Bureau, who have added offensive comments against human rights activists.[53] The websites of Shiite and opposition groups, and even of public entities like the University of Bahrain and the Department of Legal Affairs, have suffered from attacks.[54] Cyber attacks against independent forums, opposition websites, and online news sources reportedly intensified in advance of the most recent elections.

[51] "Case Regarding Publication of Names of National Security Employees Postponed to May" [in Arabic] *Alwasat*,, April 19, 2010, http://www.alwasatnews.com/2782/news/read/404013/1.html.

[52] Reporters Without Borders, "Countries Under Surveillance: Bahrain."

[53] Bahrain Youth Society for Human Rights, "Bahraini Authorities Block Websites that Criticize Government Policies," news release, August 08, 2007, http://bahrainrights.hopto.org/en/node/1373.

[54] "Lawsuit on Hacking of the University of Bahrain Website Rejected by Court," [in Arabic] Alwasat, March 18, 2010, http://www.alwasatnews.com/2750/news/read/382665/1.html; See also "Website of the Department of Legal Affairs is Hacked" [in Arabic] *Albilad*, November 21, 2009 http://www.albiladpress.com/news_inner.php?nid=27387&cat=1.

BELARUS

	2009	2011
INTERNET FREEDOM STATUS	n/a	Not Free
Obstacles to Access	n/a	19
Limits on Content	n/a	23
Violations of User Rights	n/a	27
Total	n/a	69

POPULATION: 9.5 million
INTERNET PENETRATION: 27 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

While the Belarusian government has promoted the use of the internet for economic purposes, the impact of the new medium in the political sphere remains limited. The authorities impose severe restrictions on all news outlets, and the security services have increasingly attempted to introduce various internet surveillance technologies. A presidential decree signed in February 2010 and subsequent regulations provide a legal basis for extensive censorship and monitoring of the internet. The government's desire to suppress the free flow of information became even more evident during, and immediately following, the December 2010 presidential election. The authorities blocked international connections to the SMPT port 465 and HTTPS port 443, preventing users from securely posting content on social media sites like Facebook, and sending secure messages through Gmail. In addition, the government created fake mirror websites to divert users from accessing independent news sources, and launched distributed denial-of-service (DDoS) attacks against the opposition sites.

Recent years have seen an increase in internet use and mobile-telephone penetration in Belarus. Some 27 percent of the population uses the internet and 93 percent of the population uses mobile phones. However, state-imposed and other infrastructural restrictions significantly constrain Belarusians' ability to fully access these technologies and related applications. Internet costs in Belarus are higher than in all neighboring countries.

OBSTACLES TO ACCESS

Access to digital media has grown significantly since it was first made available to the public in 1993, but widespread poverty and poor infrastructure, particularly in rural and peripheral areas, remain barriers to access. According to the 2009 figures by the International Telecommunications Unions, there were 2.6 million internet users in Belarus, for a penetration rate of 27 percent,[1] although some local sources put that number at 3.7 million as of May 2010.[2] The majority of users are young people, with those aged 15–24 making up 37.2 percent and those aged 25–34 accounting for 28 percent. Just 3.5 percent of Belarusian users are aged 55 and over.[3] In December 2010, more than 49 percent of users reported having broadband access, while 18.7 percent reported using dial-up and 5.6 percent used mobile-phone connections.[4] The key divide in levels of access is not so much between rural and urban populations—since some 70 percent of Belarusians live in urban areas—as between Minsk and other parts of the country. In Minsk there are 62 computers per 100 households,[5] compared with 40 per 100 households in the country as a whole.[6]

The cost of broadband access via DSL and cable is generally tied to volume, reflecting the pricing structure that Beltelecom, the state-owned telecommunications monopoly, uses when selling bandwidth to downstream internet-service providers (ISPs). This makes it expensive to download large items like music or movies, but for common activities like e-mail and web browsing, the volume surcharges do not form a barrier for most users. Though unlimited internet access service was launched by Beltelecom in 2007, it is still rather expensive and is not widely available.

Over 90 percent of users regularly access the internet at home, and 28 percent do so at work; only 4.5 percent regularly use the internet at school. Cybercafes are the least popular point of access, with just 3.66 percent using them often.[7] There are currently 1,262 public internet-access points in Belarus, all of which are provided by Beltelecom.[8] As of the

[1] International Telecommunications Union (ITU), "ICT Statistics 2009— Internet,"http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#, accessed February 23, 2011.
[2] "В Беларуси более 470 тыс. пользователей широкополосного интернет-доступа" [There are more than 470 thousand broadband internet users in Belarus], It.tut.by, April 22, 2009, http://it.tut.by/news/94161.html.
[3] Mikhail Doroshevich,"Internet in Belarus, December 2010," E-Belarus.org, February 4, 2011, http://www.e-belarus.org/news/201102041.html.
[4] M. Doroshevich,."Internet in Belarus, February 2010," E-Belarus.org, April 5, 2010, , http://www.e-belarus.org/news/201004051.html ; "Цифры ИТ – статистика в Беларуси" [IT figures - statistics for Belarus] , IT.tut.by, http://it.tut.by/numbers.html, accessed February 25, 2011.
[5] "На 100 столичных семей приходится 62 персональных компьютера" [62 personal computers for 100 households in the capital city], It.tut.by ,October 30, 2009, http://it.tut.by/news/92302.html.
[6]"На 100 домашних хозяйств в Беларуси приходится 40 компьютеров" [40 personal computers for 100 households in Belarus], It.tut.by, March 25, 2010, http://it.tut.by/news/90590.html.
[7] Doroshevich, "Internet in Belarus, December 2010."
[8] "Цифры ИТ – статистика в Беларуси" [IT figures–statistics for Belarus]

end of 2010, the country's four mobile phone service providers had approximately nine million subscribers combined, for the total penetration rate of 93 percent.

There is a high level of government involvement in the electronic communications sector, and there is no independent regulator, as the Ministry of Communications and Information Technology handles regulatory functions. Beltelecom maintains a monopoly on international data transfers, and the fees it charges local ISPs for bandwidth exceed by a factor of three the cost at which operators in neighboring Baltic countries can buy bandwidth; the ISPs must recoup this cost from customers, who resort to sharing connections through the creation of neighborhood-level local area networks (LANs).

The Ministry of Communications and Information Technology has issued 180 licenses for secondary internet providers. However, only 35 active secondary ISPs currently operate in Belarus, and Beltelecom's subsidiary Belpak remains the largest ISP. There are also four mobile-phone operators offering internet access.[9] In 2009, ISPs were allowed to provide wireless broadband access; before that, only Beltelecom provided WiFi internet access. The company had already installed by that time over 210 access points. More than 130 of them were situated in Minsk, while others were in regional centers, and some were in district centers.[10]

Various Web 2.0 applications such as the social networking site Facebook, video-sharing site YouTube, and microblogging service Twitter are slowly gaining in popularity. However, as of the end of 2010, less than five percent of internet users accessed Facebook regularly. Significantly more popular is the Russian social networking utility VKontakte, which is the third most accessed site in Belarus.[11] During the December 2010 elections, the government temporarily disrupted access to social-networking applications and services such as Facebook, YouTube, and Gmail, in efforts to prevent citizens from sharing videos of protests, hinder their capacity to connect and organize, and impede the political opposition from sending secure emails to their supporters.

The State Center for Information Security, under the supervision of the president and initially a unit of the special security service (KGB), is a specialized body responsible for protecting state secrets. The center also manages the administration of the country's top-level domain (.by). For much of 2009, there were 20,000 domains in the .by zone. The price for an initial year's registration is 130,000 Belarusian rubles (US$43), and continuation costs 95,000 rubles (US$32).[12]

According to regulations that followed Presidential Decree No. 60 of February 1, 2010, all legal persons' sites in the .by domain are now obliged to use Belarusian hosting

[9] "Цифры ИТ – статистика в Беларуси" [IT figures–statistics for Belarus]
[10] Doroshevich, "Internet in Belarus, February 2010."
[11] Alexa, "Top Sites in Belarus," http://www.alexa.com/topsites/countries/BY, accessed February 22, 2011.
[12] "Цифры ИТ – статистика в Беларуси" [IT figures-statistics for Belarus.].

services.[13] This rule does not apply to sites belonging to physical persons. However, a physical person's site that is hosted on a national hosting provider, including internet resources providing free hosting, is subject to compulsory registration carried out by the ISP. Moreover, government officials have announced that submission of false registration information will bring legal repercussions.

LIMITS ON CONTENT

Presidential Decree No. 60 of 2010 introduced for the first time mechanisms by which ISPs are required to block access to restricted information, such as pornography or material that incites violence, when it is sought by users. Enforcement of the decree is overseen by the presidential administration's Operational and Analytical Center (OAC).[14] The presidential decrees on the internet and the OAC gave rise to debates on filtering and freedom of speech on the internet,[15] but they also threatened to increase costs for ISPs, which must install filtering equipment and software. In June 2010, the Ministry of Telecommunications and the OAC issued a regulation that calls for the creation of two lists cataloging URLs of all websites that should be blocked; one list is open to the public, whereas the other list is accessible only by ISPs.[16] As of the end of the year, the publicly accessible list did not contain any URLs.[17]

Presidential Decree No. 60 was only a prelude to suspected blocking and technical hijacking of independent and opposition websites that occurred on December 19, 2010 the date of presidential elections, and the following day. For example, the sites of the news outlets Charter97 and Belarus Partisan were temporarily inaccessible during the two day period. Internet users were also sporadically unable to access a host of international websites such as Facebook, LiveJournal, and YouTube. Deep-packet inspection, used in some countries such as China and Iran to monitor and filter unwanted content, has not been used so far. However, a capability for deep-packet inspection was included in Beltelecom's tender call for broadband remote-access servers.

[13] Decree of the Council of Ministers No. 644 of April 29, 2010, "On Some Questions of Improving Usage of the National Segment of the Global Internet Computer Network."
[14] Decree of the President of Belarus No. 60 of February 1, 2010, available in Russian at http://www.mininform.gov.by/documentation; "Decree on Internet Limitations Prepared in Belarus (Text of the Document)", Charter 97, December 14, 2009, http://www.charter97.org/en/news/2009/12/14/24572/.
[15] "Положение о порядке взаимодействия операторов электросвязи с КГБ и ОАЦ утверждено указом №129 от 3 марта 2010 года" [Regulations on electronic communications providers cooperation with the KGB and OAC introduced by the Decree No129, March 3, 2010], Telegraf.by, March 10, 2010, http://telegraf.by/2010/03/polnij-tekst-polozhenija-o-dostupe-k-abonentskim-bazam-operatorov-svjazi.html.
[16] "БелГИЭ приступила к формированию "черного списка" [State Supervisory Body for Telecommunications Started Forming the "Black List"] Electroname, July 9, 2010, http://www.electroname.com/story/7329.
[17] "Списки ограниченного доступа" [Lists of Restricted Access], Ministry of Telecommunications, http://belgie.by/node/216, accessed on February 20, 2010.

Even before Presidential Decree No. 60, the government engaged in ad hoc efforts to limit access to certain content deemed contrary to its interests. For example, a number of opposition websites and independent media were blocked during the presidential election of September 2001. Similarly, access to a website containing cartoons about President Alyaksandr Lukashenka was blocked in August 2005.[18] Beltelecom typically cited technical problems for the blockages.[19] In addition, Russian gay and lesbian websites were blocked since 2005 at the order of a government commission tasked with combating pornography and violence, marking the only case of a formal decision to block particular content.

Self-censorship has become a pervasive phenomenon for both traditional and web-based media. Like their counterparts working for print outlets, television, and radio stations, online commentators and administrators of web portals avoid posting content that could put them at odds with the government. Moreover, the government uses indirect economic pressure to undercut financial support for certain sites. There is an unofficial blacklist of independent online outlets, and major advertising companies are advised not to place their ads on these sites.

In 2005 the popular Belarusian portal TUT.BY refused to put up banners advertising opposition websites. It is unknown whether this was a result of pressure from the authorities or merely an attempt by the site to protect its business.[20] In 2009, TUT.BY tightened control over discussion forums by employing moderators to screen comments before they are posted. The portal's owner claimed that the new policy, which applied only to news discussions, was simply aimed at blocking vulgar language and other such disruptions.[21]

Print outlets, television, and radio continue to be the main sources of news and information for most Belarusians, though there are increasing efforts to extend mainstream news to online platforms. Traditional media still have a much stronger presence in society than new media, and the internet is viewed more as a source of entertainment or as a place to state contesting opinions. However, web-based independent media played a much more visible role and attracted larger readership in advance of the 2010 elections than previously.

While the potential role of information and communication technologies (ICTs) in election campaigning in Belarus was understood as early as 2001, it was only in 2006 that the use of the internet during elections became visible. Blogs, forums, LiveJournal online communities, and so-called flash mobs—public gatherings organized via ICTs—were prominent features of the 2006 presidential election campaign. Independent online sources managed to compete with state-controlled newspapers, radio, and television, at least for the minority who had occasional access to internet. Unfortunately, although popular, blogs do

[18] Mikhail Doroshevich, "Internet Filtering in Belarus," E-Belarus.org, March 20, 2006, http://www.e-belarus.org/news/200603201.html.
[19] Mikhail Doroshevich, "Gays and Lesbians Web-sites Blocked in Belarus," E-Belarus.org, January 31, 2005, http://www.e-belarus.org/news/200501311.html.
[20] "Country Profiles: Belarus," OpenNet Initiative, May 9, 2007, http://opennet.net/research/profiles/belarus.
[21] Mikhail Doroshevich, "TUT.BY Premoderates Forums," E-Belarus.org, January 22, 2009, http://www.e-belarus.org/news/200901221.html.

not have a major influence on political life. There is little information on the use of mobile-phone text messaging, or short-message service (SMS), in political agitation. Supporters of opposition presidential candidates used SMS to mobilize people to participate in national elections in 2006, [22] although this method was not extensively used in 2010.

There have been some successful cases of online information and activism campaigns. In 2007, Belarusian blogger Yevgeny Lipkovich pushed the government to resume production of low-fat kefir in Minsk.[23] In 2008, discussions in the blogosphere prompted legislators to take notice of the illegal practices of Belarusian traffic police, and the courts took action in response.[24] There was one case in 2009 in which an online community announced itself as a political movement, but there have been no further signs of any activity by the group.[25]

Because Belarusian users have access to most online resources under ordinary circumstances, they generally do not employ proxy servers and other circumvention tools, leaving them vulnerable during the politically sensitive periods when many ad hoc disruptions occur. Most often, people are reminded about blocking only when it happens.[26] The most popular circumvention tools are proxies and TOR.[27] The main educational proxy server, sofia.niks.by, reportedly limits access to sites with illegal or erotic content, but students are able to bypass the restrictions using other proxies and tools.[28]

VIOLATIONS OF USER RIGHTS

Civil rights, including the right to access information and freedom of expression, are guaranteed by the Belarusian constitution, although they remain severely restricted in practice. A 2008 law identified online news outlets as "mass media," and Article 33 requires every such website to include the names of the publication, its founder(s), and its chief

[22] "АГП: Правакацыйныя ўлёткі ніхто не зрывае" [UCP: nobody tears off provocative leaflets], Naviny.by, March 18, 2006, http://www.nn.by/index.php?c=ar&i=882&p=1&c2=calcym&combo_calmonth=1&combo_calyear=2009.

[23] "Блогер выиграл битву за кефир!" [Blogger has won the kefir battle], Tut.by, January 27,2007, http://news.tut.by/it/100534.html; "Эпическая битва Липковича за обезжиренный кефир" [Lipkovich's Epic Battle Over Kefir," blog, November 26, 2007, http://angry-boar.livejournal.com/54957.html.

[24] "Скандал вокруг «живого щита»" [The scandal around 'human shields"], Navuny.by, October 30,2008, http://naviny.by/popular/ic_popular_240_99/; "Гаишники, устроившие «живой щит», показали лица" [Road policemen showed their faces], Kp.ru, April 19, 2008, http://kp.ru/daily/24084/317576/.

[25] Mikhail Doroshevich, "Belarus: Virtual Community Moves to Real World," E-Belarus.org, October 1, 2009, http://www.e-belarus.org/news/200910011.html.

[26] "ЖЖ заблокировано" [LJ is blocked],Community.livejournal.com/minsk_by, January 10, 2008, http://community.livejournal.com/minsk_by/4402235.html.

[27] "Как обойти блокировку сайта?"[How to circumvent a website blockade?], Charter 97, January 18, 2008, http://www.charter97.org/be/news/2008/1/18/3107/.

[28] "Байнет отдыхает: в гроднонете вводится цензура" [Bynet is having a rest, Grodnonet is being censored], Blog Grodno, November 22, 2006, http://s13.ru/archives/327.

editors, as well as the full address of the editorial office and the registration number.[29] Formally, there are no laws assigning criminal penalties or civil liability specifically for online activities, but internet activities can be prosecuted under laws applicable to mass media—mainly for defamation—or under any relevant criminal law. In addition, government officials have stressed the need to hold site owners and service providers legally accountable for illegal content, and to provide them with the tools to block such content.[30]

According to informal rules and practices, ISPs are obliged to give the authorities statistical data—separated by user—about site visits, traffic, and other topics. Mobile-phone companies are required to turn over similar data when asked by the government. Individuals are not required to register when they buy a mobile phone, but registration is needed to buy a SIM card and obtain a number.

Surveillance of cybercafes was stepped up in 2007. Under new regulations adopted by the cabinet in February of that year,[31] cafe owners must keep a 12-month history of the domain names accessed by users. State officials are authorized to review the log under conditions defined by legislation, and internet cafe managers must inform law enforcement bodies of suspected legal violations. Cybercafes are not allowed to use programs propagating violence, cruelty, or pornography, or to disseminate forbidden information. In July 2008, the head of the government's high-tech crimes department reportedly warned cybercafe owners of their responsibility for messages sent by their customers.[32] Additionally, Presidential Decree No. 60 calls for mandatory identification of users at internet cafes.

In general, it is difficult to gauge the extent to which Belarusian security services monitor internet and mobile-phone communications, but the surveillance is believed to be far-reaching. Those who engage in political activities avoid using e-mail accounts on Belarusian mail services. Many activists believe that members of the unregistered youth movement Zubr and the independent electoral observers' group Partnership have been arrested because their e-mail correspondence was intercepted. There have also been a few cases in which personal entries in the popular blog system LiveJournal were hacked, and members of the special services are known to monitor popular online forums and communities. People who are concerned about surveillance also avoid using messaging services that use open protocols, like ICQ. There are even some who suspect that the

[29] Law of the Republic of Belarus No. 427 of July 7, 2008, "On the Facilities of Mass Information," available in Russian at http://www.mininform.gov.by/documentation ; "Экспертыза новага закона «Аб СМІ»" [Analysis of the New Law on mass media], Belarusian Association of Journalists, http://baj.by/m-p-viewpub-tid-12-pid-5.html, accessed on July 9, 2010; "International analysis of the Belarusian draft Law on information, informatization and information protection," E-Belarus.org, March, 2007, http://www.e-belarus.org/article/infolaw.html.

[30]" Пролесковский знает, как зачистить интернет" [Proleskovsky knows how to clean up internet], Belaruspartisan.org, June 4, 2008, http://www.belaruspartisan.org/bp-forte/?page=100&news=25145.

[31] "Совет Министров Республики Беларусь Положения о порядке работы компьютерных клубов и Интернет-кафе" (Council of Ministers of the Republic of Belarus. Regulations on computer clubs and internet cafe functioning), Pravo.by, April 29, 2010, http://pravo.by/webnpa/text.asp?start=1&RN=C20700175.

[32] Mikhail Doroshevich, "Belarusian government adopts regulations on computer clubs and internet cafes", E-Belarus.org, February 15, 2007, http://www.e-belarus.org/news/200702151.html.

authorities secretly ask ISPs to change certain ADSL users' address distribution from dynamic to static, allowing easy monitoring. Security services routinely use legal and extralegal means to collect internet and mobile-phone users' records from ISPs, cybercafes, and mobile-phone companies in the course of their investigations. On the day of the December 2010 election, the government blocked international connections to ports 443 and 465, thereby preventing users from securely sending e-mails and posting messages on social networking sites. In addition, mobile-phone providers reportedly assisted the authorities in tracking down opposition activists.

Armed with such information, it is much easier for the regime to harass or jail a particular writer, or to hack or restrict access to a certain website, than to introduce large-scale content filtration. There have been a number of cases of arbitrary prosecution based on online journalistic activities. In 2005, a Grodno forum was "closed" by authorities because forum visitors were critically discussing the Belarusian president and his policies.[33] In 2006, creators of satirical online cartoons on the president and politics were prosecuted under criminal law and had to flee the country.[34] In August 2007, Andrei Klimau, a member of the opposition United Civic Party, was sentenced to two years in prison for calling for the overthrow of Lukashenka's regime in an online article.[35] Owners of the United Civic Party website were sued by a government official who claimed damage to his reputation because of an article on the site that accused his son of misdeeds.[36]

Most recently, several lawsuits were brought against Charter97, a pro-opposition news site based in Minsk. In March 2010, the KGB raided the website's office and confiscated the computer equipment. A suit against the outlet was brought up the same month, but later dismissed. However, the outlet was the subject of another lawsuit initiated on December 8, apparently based on the materials discovered during the March raid, although the prosecutors refused to reveal under which law the case would be prosecuted. During the year, the authorities also opened a criminal case against Charter97 alleging the publication's liability for objectionable comments posted by its readers.[37] Finally, in the wake of the election crackdown on journalists and activists, Charter97 editor Natallya Radzina was detained on December 20 by the KGB and held without official charges and without access to an attorney.[38] She was still in detention as of December 31.

[33] Mikhail Doroshevich, "Internet Forum Closed Down in Grodno," E-Belarus.org, March 14, 2005, http://www.e-belarus.org/news/200503141.html.
[34] After fleeing the country, they established an open democratic discussion platform at http://www.3dway.org.
[35] "АНДРЕЙ КЛИМОВ, ПОЛИТЗАКЛЮЧЕННЫЙ" [Andrei Klimov, political prisoner], Charter 97, August 16, 2007, http://www.charter97.org/r/index.phtml?sid=3&did=aklimov.
[36] "Суд по иску к ОГП состоится 15 августа" [The trial of UCP set for August15], UCPB.org, August 10, 2007, http://www.ucpb.org/?lang=rus&open=15135.
[37] "Против сайта charter97.org возбуждено третье уголовное дело" [Criminal case brought against charter97.org website], Electroname, December 8, 2010, http://www.electroname.com/story/9100.
[38] "Belarus Arrests, Sentences Journalists in Crackdown," Committee to Protect Journalists (CPJ), December 20, 2011, http://www.cpj.org/2010/12/belarus-arrests-sentences-journalists-in-crackdown.php.

Online activists and web-based journalists face extralegal harassment, mostly in the form of phone calls or intimidating messages. However, until 2010, physical attacks were not common. For that reason, the death of the founder of Charter97Aleh Byabenin prompted many questions among his colleagues and fellow journalists. Byabenin was found hanged from a stairway at his summer home in September 2010. Although the authorities declared his death a suicide, most independent sources questioned the official version and suspected foul play.

Technical attacks are becoming increasingly common. For example, a number of opposition and other sites were rendered inaccessible on January 10, 2008, the day of a protest by entrepreneurs, but Beltelecom officials denied involvement.[39] In April 2008, several websites run by Radio Free Europe/Radio Liberty were attacked for more than two days surrounding the 22nd anniversary of the Chernobyl nuclear disaster.[40] Most recently, in the wake of the 2010 elections, many pro-opposition sites suffered DDoS attacks. In addition, Belpak was redirecting users who tried to access certain independent media sites to copies of those sites run by pro-government actors. For example, when a user requested to access www.gazetaby.com, the ISP hijacked the request and redirected the user to www.gazetaby.in.[41] The mirror sites were almost identical to the original, but in some instances posted incorrect information, such as the location of an opposition gathering in efforts to mislead those planning to attend.

In light of the government's widespread use of technical attacks during elections, it is important to note that Belarusian criminal law actually prohibits such activity. Specifically, Article 351 of the criminal code, covering "computer sabotage," stipulates that the premeditated destruction, blocking, or disabling of computer information, programs, or equipment is punishable by fines, professional sanctions, and up to five years in prison.[42] According to Ministry of Internal Affairs data, there was a 33 percent growth in cybercrime in 2009 compared with 2008.[43] The government has stated its intention to accede to the Council of Europe's Convention on Cybercrime, but it has made no moves to accede to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

[39] Mikhail Doroshevich, "Cybercrime in Belarus in the Beginning of 2008," E-Belarus.org, January 11, 2008, http://www.e-belarus.org/news/200801111.html.

[40] Hampton Stephens, "Belarusian Cyber Attack", World Politics Review, April 28, 2008, http://www.worldpoliticsreview.com/trend-lines/2012/belarusian-cyber-attack.

[41] Hal Roberts, "Independent Media Sites in Belarus Reportedly Hijacked During Election," The Berkman Center for Internet and Society, December 19, 2010, http://blogs.law.harvard.edu/hroberts/2010/12/19/independent-media-sites-in-belarus-reportedly-hijacked-during-election/.

[42] "«Белтелеком»: Возможно, независимые сайты блокировали другие организации" [Beltelecom: independent websites could be blocked by other organizations], Charter 97, January 10, 2008, http://www.charter97.org/ru/news/2008/1/10/2905/.

[43] "Количество киберпреступлений в Беларуси увеличилось" [The growth of cybercrime in Belarus], It.tut.by, January 25, 2010, http://it.tut.by/news/91330.html.

BRAZIL

	2009	2011
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access	9	7
Limits on Content	8	7
Violations of User Rights	13	15
Total	**30**	**29**

POPULATION: 193.3 million
INTERNET PENETRATION 2009: 39 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

For a country with large social and economic disparities, Brazil has made significant gains in expanding internet access and mobile-phone usage in recent years. As of 2009, it was home to the largest population of internet users in Latin America and the fourth largest in the world.[1]

The country first connected to the internet in 1990, and connectivity is now available in most areas through a variety of technologies, though some infrastructural limitations remain.[2] Several legal and judicial actions threatened free online expression in 2009 and 2010. There is an ongoing trend in which private litigants and official bodies sue internet-service providers (ISPs) and other internet companies, such as Google, and send take-down notices to blogging and social-networking platforms, such as Orkut. However, pending legislation would formalize an appeals process for such actions.

In recent years, civic participation through internet media has increased, including in response to the proposed Civil Rights Framework for the Internet in Brazil.[3] Moreover,

[1] International Telecommunications Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

[2] Robert Hobbes Zakon, "Hobbes' Internet Timeline v8.2," Zakon Group LLC, http://www.zakon.org/robert/internet/timeline/, accessed August 11, 2010; Tadao Takahashi, ed., *Sociedade da Informação no Brasil: Livro Verde* [Information Society in Brazil: Green Book] (Brasilia: Ministry of Science and Technology, September 2000), http://www.mct.gov.br/index.php/content/view/18878.html; National Education and Research Network (RNP), "Mapa do Backbone" [Map of Backbone], http://www.rnp.br/backbone/index.php, accessed August 11, 2010.

[3] Maira Magro, "Cries of Censorship Lead Brazil to Alter Internet Bill," *Journalism in the Americas* (blog), May 4, 2010, http://knightcenter.utexas.edu/blog/?q=en/node/7104.

restrictions on political campaigning via social-networking websites that were imposed ahead of the 2008 elections were removed for the run-up to the 2010 polls.

OBSTACLES TO ACCESS

According to the International Telecommunication Union (ITU), Brazil had over 75 million internet users as of 2009, accounting for 37 percent of the population.[4] However, penetration varies greatly among regions due to a lack of infrastructure that affects large segments of the population in rural areas.[5] For instance, while the household penetration rate is 31.5 percent in the southeast, it is only 10.6 percent in the north. In addition, the cost of broadband access is prohibitively expensive for many Brazilians, amounting to about 5 percent of per capita income.[6] Broadband access is increasing as prices fall, reaching 7 percent of the population in 2009,[7] but the market is still concentrated among major telecommunications and cable companies.[8] In addition, Brazil is currently the largest mobile-phone market in Latin America, and penetration is rapidly increasing. Statistics show an average annual increase of 18 percent in the rate of mobile-phone use over the last five years, with approximately 197 million mobile phones in use by November 2010.[9]

Great improvements have been made in recent years as the government has initiated dozens of programs to connect the population to the internet, including investment in WiMax networks, Digital Cities projects,[10] and a series of regional projects focused on media literacy and digital inclusion.[11] Many of these programs employ broadband

[4] International Telecommunications Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

[5] Brazilian Institute of Geography and Statistics (IBGE), "Síntese de Indicadores 2008" [Synthesis of 2008 Indicators 2008], http://www.ibge.gov.br/home/estatistica/populacao/trabalhoerendimento/pnad2008/default.shtm, accessed June 5, 2010.

[6] Institute of Applied Economic Research (Ipea), *Comunicados do Ipea No. 46: Análise e recomendações para as políticas públicas de massificação de acesso á internet em banda larga* [Ipea Communiqué No. 46: Analysis and Recommendations for Public Policy on Expansion of Access to Broadband Internet] (Brasilia: Ipea, April 2010), p. 3 and 9 http://agencia.ipea.gov.br/images/stories/PDFs/100426_comunicadodoipea_n_46.pdf.

[7] Ministry of Communications, *Um Plano Nacional para Banda Larga: O Brasil em Alta Velocidade* [A National Plan for Broadband: Brazil in High Speed] (Brasilia: Ministry of Communications, 2010), http://www.mc.gov.br/wp-content/uploads/2009/11/o-brasil-em-alta-velocidade1.pdf; International Telecommunication Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx.

[8] Teleco, "Seção: Banda Larga—Market Share de Banda Larga no Brasil" [Section: Broadband—Market Share of Broadband in Brazil], http://www.teleco.com.br/blarga.asp, accessed August 11, 2010.

[9] Teleco, "Seção: Telefonia Celular—Estatísticas de Celulares no Brasil" [Section: Cellular Telephony—Statistics of Cellular Telephones in Brazil], December 29, 2010, http://www.teleco.com.br/ncel.asp.

[10] Redline Communications Inc., "Neovia and Redline Initiate US$30 Million WiMAX Network in Brazil," WiMAX Industry, August 2, 2007, http://www.wimax-industry.com/pr/7p.htm; for a list of Digital Cities, see Teleco, "Seção: Banda Larga—Cidades Digitais no Brasil" [Section: Broadband—Digital Cities in Brazil], July 28, 2008, http://www.teleco.com.br/cidadesdigitais.asp.

[11] For a complete list, see Brazilian Institute of Science and Technology (IBICT), "Iniciativas no Brasil" [Initiatives in Brazil], http://inclusao.ibict.br/index.php/iniciativas-no-brasil.

technology, and in 2010 the government launched the National Broadband Plan, which aims to triple broadband access by 2014.[12] Internet access has also been boosted by a proliferation of privately owned "LAN (local area network) houses," in which small entrepreneurs have purchased multiple computers via a government loan program, then offered access at reasonable prices for users. In many regions, these sites have become the primary means of internet access. Research published by the Brazilian Internet Steering Committee in 2008 showed that nearly 80 percent of the people from the lowest income brackets who access the internet do so via commercial venues such as LAN houses, a dramatic increase from 48.08 percent in 2006.[13]

Some states and cities have approved laws establishing limits on youths' use of public computers in LAN houses. In São Paulo state, minors under the age of 16 can only use LAN houses with the written authorization of their parents, while in the city of Ilha Solteira, a court order prohibited teenagers from visiting LAN houses.[14] As Brazilians at all socioeconomic levels use the internet,[15] a growing number have taken advantage of the country's e-commerce, e-government, and online-banking services, which are among the most developed in the world.[16] Unlike in previous years, there were no instances during 2009 or early 2010 of advanced web applications like the video-sharing site YouTube or the social-networking platform Orkut being completely blocked by court orders, though individual videos or comments have been removed.

Despite an intricate regulatory environment, no specific legal or economic obstacles restrict the operation of ISPs or other businesses providing access to digital technologies. However, privatization plans implemented in the 1990s have created a trend toward concentration in the telecommunications market, and in the ISP market specifically. While more than 1,000 ISPs now operate in the country,[17] the four largest companies—Brasil

[12] Ministry of Communications, *Um Plano Nacional para Banda Larga*.
[13] Center of Studies on Information and Communication Technologies (CETIC), "TIC Domicílos e Usuários 2008—Total Brasil" [Statistics on Home Internet Access and Users 2008—Total Brazil], September/November 2008, http://www.cetic.br/usuarios/tic/2008-total-brasil/rel-int-04.htm; CETIC, "TIC Domicílios e Usuários 2006" [Statistics on Home Internet Access and Users 2006], July/August 2006, http://www.cetic.br/usuarios/tic/2006/rel-int-04.htm; Paula Góes, "Brazil: Socio-Digital Inclusion Through the Lan House Revolution," Global Voices, September 28, 2009, http://globalvoicesonline.org/2009/09/28/brazil-socio-digital-inclusion-through-the-lan-house-revolution/; Colin Brayton, "Brazil: Tupis Are In The LAN House," *The New Market Machines* (blog), March 16, 2008, http://cbrayton.wordpress.com/2008/03/16/brazil-tupis-are-in-the-lan-house/.
[14] Felipe Zmoginski, "Justiça proíbe menor de ir à LAN House em SP" [Justice Prohibits Minor from Going to LAN House in São Paulo], INFO Online, April 27, 2009, http://info.abril.com.br/noticias/tecnologia-pessoal/justica-proibe-menor-de-ir-a-lan-house-em-sp-27042009-39.shl.
[15] Marcelo Ballvé, "In Brazil, Internet Access Grows Rapidly, Even Among Poor," World Politics Review, April 3, 2008, http://www.worldpoliticsreview.com/article.aspx?id=1891.
[16] "Brazil—Internet and Broadband Market," Research and Markets, December 2008, http://www.researchandmarkets.com/reportinfo.asp?report_id=680153.
[17] Teleco, "Seção: Banda Larga—Provedores de Acesso à Internet – Outros Provedores" [Section: Broadband—Internet Access Providers – Other ISPs], May 14, 2010, http://www.teleco.com.br/blarga_pprov.asp.

Telecom, POP, Terra, and UOL—control more than 50 percent of the market.[18] Seven private companies share the mobile-phone market, of which the largest four control over 99 percent.[19]

The National Telecommunications Agency (ANATEL) and the Administrative Council for Economic Defense (CADE), an antitrust body, work to ensure that information and communication technologies (ICTs) operate in a free, fair, and independent manner. The two agencies have a cooperation agreement that defines their competencies. The CADE is authorized by the General Telecommunications Law to have the final word when dealing with antitrust issues, such as market concentration and price setting.[20] In a pioneering initiative, the Brazilian Internet Steering Committee, a multi-stakeholder organization, was created in 1995 to guarantee transparency and social participation in decisions related to internet governance.[21] Committee members come from the government, the private sector, academia, and nongovernmental organizations, with the last group chosen since 2004 in relatively democratic and open elections.

LIMITS ON CONTENT

The government does not employ any technical methods to filter or otherwise limit access to online content. Nonetheless, legal action by the judiciary and government officials has emerged in recent years as a possible barrier to free speech and a means of removing content that is deemed undesirable.

It is increasingly common for civil and administrative charges to be filed against ISPs, online news journals, and bloggers. Google Brazil and some of its services, such as Orkut and YouTube, have been the target of numerous judicial demands,[22] some of which have involved the removal of content that would be a matter of public interest. In a groundbreaking decision in February 2009, a judge obliged Google to change its search results in Brazil with regard to a Brazilian businessman.[23] Other rulings ordered the closure of e-mail and blog accounts, and the deletion of pages from Orkut to protect individuals'

[18] Teleco, "Seção: Banda Larga—Provedores de Acesso à Internet" [Section: Broadband—Internet Access Providers], May 14, 2010, http://www.teleco.com.br/internet_prov.asp.
[19] Teleco, "Seção: Telefonia Celular—Operadoras de Celular, Jun/10" [Section: Cellular Telephony—Cellular Operators, June 2010], August 5, 2010, http://www.teleco.com.br/opcelular.asp.
[20] Maria Cecília Andrade, Ubiratan Mattos, and Pedro C. E. Vicentini, "Reforms in Brazilian Telecommunications Regulations and their Impact on Sector Competition," in *The Antitrust Review of the Americas 2009* (London: Global Competition Review, 2009), http://www.globalcompetitionreview.com/reviews/9/sections/31/chapters/361/reforms-brazilian-telecommunications-regulations-impact-sector-competition; Teleco, "Regulation: Legislation Guide," July, 28, 2010, http://www.teleco.com.br/en/en_legis.asp.
[21] See the website of the Brazilian Internet Steering Committee, http://www.cg.org.br/internacional/index.htm.
[22] Danny O'Brien, "Is Brazil the Censorship Capital of the Internet? Not Yet," *CPJ Blog*, April 28, 2010, http://cpj.org/blog/2010/04/is-brazil-the-censorship-capital-of-the-internet.php.
[23] Alessandro Cristo, "Justiça discute permanência de notícias na internet" [Justice Discusses How to Keep News Online], Consultor Jurídico, March 21, 2009, http://www.conjur.com.br/2009-mar-21/justica-decide-noticias-ficaram-velhas-internet.

"Right of Publicity" (their right to control how their name and image is used), to combat pedophilia, or to limit copyright infringements. In April 2010, Google began publishing a list of the countries whose government agencies send the most requests for content removal or data disclosure; Brazil topped the list with 291 in December 2009, an increase from 2008.[24] According to Brazilian legal experts, the take-down notices and other orders generally stem from private legal disputes rather than direct demands from the government.[25]

Upon receipt of a take-down notice, ISPs and other companies are expected to remove the content, but the affected user may then challenge the removal in court. Some free expression groups have argued that this system, which effectively places the legal burden on the owner, producer, or host of the censored content and allows only after-the-fact remedies, leaves room for abuse and suppression of critical speech. The current practice has developed somewhat informally and is not established by law, but Congress is considering legislation that would codify it.[26]

Past state-initiated censorship attempts have primarily appeared in the context of elections. However, in a positive development, following strong political pressure, the Senate in September 2009 approved changes to the electoral law that permitted the use of the internet in political campaigns. The Superior Electoral Court had prohibited online campaigning during the 2008 elections.[27] The new law, No. 12.034/09, protects freedom of speech. It also stipulates that election propaganda over the internet would be permitted after July 5, 2010, the same date when paid advertisements on radio and television were authorized to begin ahead of October general elections; any premature advertising could result in sanctions. Candidates are also permitted to campaign through social networks, instant messaging, and the Twitter microblogging service, but the content must be generated or edited by candidates, parties, or coalitions. While ordinary citizens are permitted to post comments in favor of candidates as a matter of their individual personal opinion, paid campaign advertisements or even free advertising on the websites of corporations or public entities are forbidden. Infractions of these campaign rules can be

[24] Google, "Government Requests," http://www.google.com/governmentrequests, accessed August 10, 2010; O'Brien, "Is Brazil the Censorship Capital of the Internet? Not Yet."

[25] Such lawsuits can be filed more easily in Brazil than in many other countries, where other forms of dispute resolution or regulation of online content prevail. See O'Brien, "Is Brazil the Censorship Capital of the Internet? Not Yet."

[26] Ibid.

[27] The court's resolution, No. 22.718, determined that electoral campaigns and advertisements could only be posted on a candidate's web page. It barred electoral campaigns from using such tools as Orkut, YouTube, e-mail, and text messaging, and prohibited them from buying advertising space on the internet. Paula Góes, "Brazil: Blogs Banned from the 2008 Elections," Global Voices, March 30, 2008, http://globalvoicesonline.org/2008/03/30/brazil-blogs-banned-from-the-2008-elections/; Superior Electoral Tribunal, Resolution No. 22.718, available at http://www.tse.gov.br/internet/eleicoes/2008/pdf/r22718.pdf; Gaurav Dua, "Orkut Brazil Warns Users Against Political Showdown Regarding Upcoming Elections," Orkut Plus, September 14, 2008, http://www.orkutplus.net/2008/09/orkut-brazil-warns-users-against-political-showdown-regarding-upcoming-elections.html.

punished with severe fines. In practice, during the run-up to the October elections, a range of candidates were indeed able to make use of social media in their campaigns.

National and international news sources are unrestricted, and Brazilians freely gather information through the internet, mobile-phone technology, and other ICTs.[28] Blogs,[29] photoblogs, social-networking platforms,[30] and citizen journalism have proliferated in recent years.[31] With 86 percent of internet users regularly connected to Orkut and other social-media sites, Brazil has the highest social-media penetration rate in the world. In 2009, social media accounted for 22 percent of Brazilians' time online.[32] As of August 2010, Orkut remained Brazil's leading social networking tool, reaching over 36 million people. However, the number of Facebook users increased dramatically from 2009 as Brazilians sought to connect with acquaintances outside the country where Orkut is less popular. Twitter's popularity also grew significantly, nearly doubling its penetration to 23 percent of internet users.[33]

There have been a host of projects aimed at improving government transparency and democratic governance via use of the internet, such as the e-Democracy project led by Congress and "Adopt a Representative," a civil society initiative to increase public supervision of local officials and participation in policymaking.[34] In addition, the government in 2009 released online many documents from the country's dictatorship period.[35] Another recent phenomenon has been the growing number of policemen who write blogs intended to build public trust. Other examples include projects promoting open access to public

[28] Maira Magro, "Journalists Exchange Experiences About Online News During Seminar in São Paulo," Knight Center for Journalism in the Americas, June 14, 2010, http://knightcenter.utexas.edu/events_article.php?page=9946.

[29] Some top-ranked Brazilian blogs are listed here: Caio Caprioli, "Os blogs mais acessados do Brasil" [The Most Accessed Blogs in Brazil], *Metablog*, May 5, 2008, http://colunistas.ig.com.br/metablog/2008/05/05/os-blogs-mais-acessados-do-brasil; "Top 100 Blogs Brasileiros Segundo o Pagerrank e os Backlinks" [Top 100 Brazilian Blogs According to Pagerrank and Backlinks], Internney, August 18, 2007, http://www.interney.net/?p=9760065.

[30] Google's Orkut is incredibly popular in Brazil. In June, Brazilians made up 48.2 percent of Orkut users worldwide. See Alexa, "Orkut.com," http://www.alexa.com/siteinfo/Orkut.com#; Matt Rhodes, "Brazil Tops League of Social Media Users," Fresh Networks, June 15, 2010, http://www.freshnetworks.com/blog/2010/06/nielsen-study-social-media-22-percent-time-online/; ComScore, "Eighty Five Percent of Brazilian Internet Users Visited a Social Networking Site in September 2008," news release, November 19, 2008, http://www.comscore.com/press/release.asp?press=2592.

[31] Brazilians are active in the Global Voices citizen journalism project, and there is a Brazilian site for user-generated content called Overmundo. See Global Voices' Brazil page at http://globalvoicesonline.org/-/world/americas/brazil/, and Overmundo at http://www.overmundo.com.br/.

[32] "Social Networks/Blogs Now Account for One in Every Four and a Half Minutes Online," *Nielsen Wire* (blog), June 15, 2010, http://blog.nielsen.com/nielsenwire/online_mobile/social-media-accounts-for-22-percent-of-time-online/.

[33] Sarah Radwanick, "Orkut Continues to Lead brazil's Social Networking Market, Facebook Audience grows Fivefold," press release, ComScore, October 7, 2010, http://www.comscore.com/Press_Events/Press_Releases/2010/10/Orkut_Continues_to_Lead_Brazil_s_Social_Networking_Market_Facebook_Audience_Grows_Fivefold/(language)/eng-US.

[34] Technology for Transparency Network, "Adote um Vereador" [Adopt a Representative], http://transparency.globalvoicesonline.org/project/adote-um-vereador.

[35] Yana Marull, "Brazil Puts Dictatorship Files on the Web," *Sydney Morning Herald*, May 14, 2009, http://news.smh.com.au/breaking-news-technology/brazil-puts-dictatorship-files-on-the-web-20090514-b3zw.html.

information and governmental data,[36] and projects tracking the quality and security of public schools through online platforms and mobile phones.

Brazilian bloggers and citizen journalists regularly take advantage of digital technologies to circulate information and mobilize protests, including surrounding natural disasters. When severe rain and mudslides occurred in Rio de Janeiro in April 2010, online activists played a critical role in providing information to the news media and the public. This included creating a collaborative map displaying various forms of damage suffered across the metropolis.[37] Mobile phones have become a major tool for organizing events like the annual gay rights parade in São Paulo, as well as a means for bringing attention to the prevalence of violent crime.

In an example of online opinion impacting policy debates, the Civil Rights Framework for the Internet in Brazil, an internet regulation bill before Congress, attracted considerable public commentary through blogs, Twitter (at #marcocivil), and other online platforms. The New York–based Committee to Protect Journalists and critics in Brazil said that the initial language in the bill would promote censorship,[38] as it allowed third parties to request content removal based on complaints of any kind. The bill's subsequent draft,[39] the result of public pressure and comments, renders web hosts liable only if they fail to comply with a direct court order to remove content, rather than requiring them to preemptively self-censor. The bill was still awaiting passage as of December 2010. Similarly widespread social participation featured in the discussions surrounding the reform of the Brazilian Copyright Act (on Twitter at #reformaLDA). Civil society groups have joined forces with academics to support or criticize the government and press for a transparent process and a more flexible copyright law.[40] There are still concerns about the bill's potential impact on internet access. It too was still pending as of December 2010, as many pieces of legislation were put on hold until after the fall elections.

[36] Maira Magro, "Brazil's Chamber of Deputies Approves Bill Granting Access to Public Information," *Journalism in the Americas*, April 14, 2010, http://knightcenter.utexas.edu/blog/?q=en/node/6940; see also the website of the civil society group Fórum de Direito de Acesso a Informações Públicas [Forum for the Right of Access to Public Information] at http://www.informacaopublica.org.br/.

[37] Maira Magro, "Brazil's Citizen Journalists Crucial in Covering Record Floods," *Journalism in the Americas*, April 9, 2010, http://knightcenter.utexas.edu/blog/?q=en/node/6900; "Veja o mapa da devastação no Rio e colabore" [View Map of Devastation in Rio and Collaborate], *O Globo*, http://oglobo.globo.com/rio/info/chuva/.

[38] Monica Tavares, "Marco da internet: sites jornalísticos querem ficar de fora do projeto do governo que regulamenta o setor" [Internet Framework: News Sites Want to Stay Out of Government Project to Regulate the Sector], *O Globo*, April 16, 2010, http://oglobo.globo.com/economia/mat/2010/04/16/marco-da-internet-sites-jornalisticos-querem-ficar-de-fora-do-projeto-do-governo-que-regulamenta-setor-916364403.asp; O'Brien, "Is Brazil the Censorship Capital of the Internet? Not Yet."

[39] Cultura Digital, "Balanço parcial: novos artigos atendem às sugestões sobre remoção de conteúdo" [Partial Balance: New Articles Meet Suggestions Regarding Content Removal," May 3, 2010, http://culturadigital.br/marcocivil/2010/05/03/balanco-parcial-do-debate-novo-artigo-20-atende-as-contribuicoes.

[40] See the website of the copyright reform movement at http://www.reformadireitoautoral.org/.

VIOLATIONS OF USER RIGHTS

The constitution and federal law protect freedom of speech as well as cultural and religious expression. Specific laws also establish freedom of the press. However, some legislation limits these rights, and the constitution outlines a particularly complex legal framework, especially regarding online speech.[41] For example, free expression of thought is assured and anonymity is formally forbidden in the same paragraph.[42] This provision is now part of the above-mentioned 2009 law that regulates elections in Brazil (Law No. 12.034/09).[43] In addition, bill 494/08, currently under consideration in the Senate, aims to impose a series of obligations on ISPs, websites, and blogs to ensure cooperation with the police on pedophilia investigations.[44] Brazil's judiciary is independent but some judges have issued rulings that may be detrimental to the full exercise of free expression online, such as a November 2009 decision forbidding bloggers in the state of Mato Grosso from reporting on embezzlement charges against a local politician.[45]

Individual bloggers have faced defamation lawsuits, sometimes for very high amounts. These are most commonly filed by companies over postings that criticize their products or services.[46] In one case, blogger Denise Bottmann was sued after posting comments and evidence accusing a publisher of plagiarism;[47] she eventually won the lawsuit in April 2010.[48] In another example, Emilio Moreno da Silva Neto, a blogger and journalism student at Colégio Santa Cecília, was ordered in November 2009 to pay his school's

[41] An English translation of the constitution is available at http://www.v-brazil.com/government/laws/constitution.html.
[42] Jose Murilo, "Brazil: Inventive Censorship, and the Case for Anonymity," Global Voices, September 7, 2008, http://globalvoicesonline.org/2008/09/07/brazil-inventive-censorship-and-the-case-for-anonymity.
[43] Law 12.034, September 29, 2009, available at http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Lei/L12034.htm.
[44] Brazilian Senate, "Tramita no Senado projeto para coibir crimes contra crianças e adolescentes na internet" [Senate Clears Project to Curb Crimes Against Children and Adolescents on the Internet], news release, May 31, 2010, http://www.senado.gov.br/agencia/verNoticia.aspx?codNoticia=102501&codAplicativo=2.
[45] Brazilian Association of Investigative Journalism (ABRAJI), "Judge forbids bloggers from writing about politician's court case," International Freedom of Expression eXchange (IFEX), November 20, 2009, http://www.ifex.org/brazil/2009/11/20/cavalcanti_and_vandoni_injunction/.
[46] Alessandro Martins, "Lista de blogs processados ou ameaçados juridicamente" [List of Blogs Sued or Threatened With Legal Action], *QueroTerUmBlog.com!*, December 17, 2009, http://queroterumblog.com/lista-de-blogs-processados-ou-ameacados-juridicamente/. In December 2010, the newspaper *Folha de São Paulo* filed a lawsuit against a blog that sought to satirize the well-known daily. ABRAJI, "Newspaper files lawsuit against satirical blog," IFEX, http://www.ifex.org/brazil/2010/12/30/falha_de_sao_paulo_sued/.
[47] Urso de Óculos, "Denise Bottmann sued by Landmark Press", March 4, 2010, http://www.ursodeoculos.com/english/?p=1315.
[48] Alessandro Martins, "O caso de processo a blog mas importante do ano" [The Year's Most Important Case of a Blog Being Sued], *QueroTerUmBlog.com!*, December 26, 2009, http://queroterumblog.com/o-caso-de-processo-a-blog-mais-importante-do-ano/. And http://apoiodenise.wordpress.com/2010/04/01/acao-de-martin-claret-contra-denise-bottmann-e-rejeitada-em-segunda-instancia-por-unanimidade/.

principal approximately US$9,200 for comments posted on his blog by an anonymous user about a fight at the school.[49]

The Digital Crimes Bill,[50] first introduced in 2005 by Senator Eduardo Azeredo, has raised concerns that it would restrict technologies like open WiFi networks, criminalize actions such as unlocking mobile phones, and oblige ISPs to record user information.[51] Following public criticism of the draft—including a petition that gathered over 150,000 signatures—discussion surrounding the bill largely subsided in early 2010 and was substituted by a public debate over the proposed Civil Rights Framework for the Internet in Brazil.[52] However, in the fall of 2010, the bill was brought back to the Congressional agenda, retaining a number of problematic provisions.[53] Its passage was pending at year's end.

Surveillance of internet activities is not a significant concern in Brazil, although government efforts to collect user data have increased in recent years, and illegal wiretapping remains a significant problem. Specific laws allow for surveillance, but only when authorized by judicial orders under due process. In 2007, the number of wiretaps was estimated at between 300,000 and 409,000, and most were conducted without a judicial order.[54] In 2009, civil courts authorized over 10,000 wiretaps.[55] A special congressional commission was established in 2009 to analyze surveillance issues. The panel's report

[49] ABRAJI, "Journalism Student Ordered to Pay Hefty Amount in 'Moral Damages' Case After Critical Comments Posted on His Blog," IFEX, December 1, 2009, http://www.ifex.org/brazil/2009/12/01/neto_sued_for_damages/; Juliana Lima, "Brazilian Journalism Student Must Pay Damages for Comment on His Blog," *Journalism in the Americas*, November 26, 2009, http://knightcenter.utexas.edu/blog/?q=en/node/5935.

[50] "Censura Não!: Brazilian Bloggers Protest New Cybercrime Bill," OpenNet Initiative, July 25, 2008, http://opennet.net/blog/2008/07/censura-n%C3%A3o-brazilian-bloggers-protest-new-cybercrime-bill; Reporters Without Borders, "Legislators Urged to Oppose Cyber-crime Bill Likely to Threaten Online Free Expression," news release, July 23, 2008, http://en.rsf.org/brazil-legislators-urged-to-oppose-cyber-23-07-2008,27917.html; Paula Góes, "Brazil: Bloggers Question the 13 New Cyber-Crimes," Global Voices, July 17, 2008, http://globalvoicesonline.org/2008/07/17/brazil-bloggers-question-the-13-new-cyber-crimes/; Rodrigo Guimarães Colares, "Brazilian Cybercrime Bill Needs More Transparency," Safernet Brasil, June 17, 2007, http://www.safernet.org.br/site/noticias/brazilian-cybercrime-bill-needs-more-transparency.

[51] Paula Martini, "Access Versus Surveillance: Brazilian Cybercrime Law Project," iCommons, November 5, 2008, http://archive.icommons.org/articles/access-versus-surveillance-brazilian-cybercrime-law-project.

[52] O'Brien, "Is Brazil the Censorship Capital of the Internet? Not Yet"; Joana Varon, "Internet and Democracy: Brazilian Procedure for a Civil-Rights Based Regulatory Framework for Internet," *a2k* (blog), January 12, 2010, http://a2kbrasil.org.br/Internet-and-democracy-Brazilian; Cultura Digital, "Draft Bill Proposition on Civil Rights Framework for Internet in Brazil," April 20, 2010, http://culturadigital.br/marcocivil/2010/04/20/draft-bill-propostion-on-civil-rights-framework-for-internet-in-brazil/.

[53] Joana Varon, "Brazilian Internet regulation: new challenges imposed by misguided cybercrime draft bill," A2K Brasil, November, 8th, 2010, http://www.a2kbrasil.org.br/wordpress/lang/en/2010/11/brazilian-internet-regulation-new-challenges-imposed-by-misguided-cybercrime-draft-bill/; "Comentários e Sugestões sobre o substitutivo do Projeto de Lei de Crimes Eletrônicos (PL n. 84/99) apresentado pela Comissão de Constituição e Justiça e de Cidadania" [Comments and Suggestions About the Replacement of the Bill on Cybercrimes (PL n. 84/99) Presented by the Commission on the Constitution, Justice and Citizenship], Rio de Janeiro School of Law, Center for Technology and Society, November 2010, http://www.a2kbrasil.org.br/wordpress/wp-content/uploads/2010/11/coment%C3%A1rios-ao-substitutivo-PL-88-99.pdf].

[54] "Trezentos mil brasileiros estão com telefone grampeado" [Three Hundred Thousand Brazilians Have Bugged Phones], Consultor Jurídico, October 27, 2007, http://www.conjur.com.br/static/text/60835,1.

[55] "Brasil tem 10,5 mil escutas telefônicas autorizadas em curso" [Brazil Has 10,500 Authorized Wiretaps Under Way], *Imprensa Livre*, May 23, 2010, http://www.redeimprensalivre.com.br/archives/5095.

suggested that many individuals, politicians, and members of the police force should be investigated and condemned for illegal wiretapping. Privacy is also threatened by defamation suits and other such cases. Brazil's recent listing by Google as the world's top issuer of requests for content removal or user information stems in part from the fact that judicial orders to remove content in private-party disputes are often accompanied by a request to identify the publisher of the information.[56]

Some lawmakers have pushed for requirements that any internet communication from a public access point, such as a LAN house, be recorded, and that data from users be gathered, to prevent crime and allow the LAN house to avoid liability for acts committed by its users. In the state of Parana, the legislature is debating a bill that would oblige LAN houses to install cameras in their computer rooms. The bill was proposed after the police department released statistics showing that 30 percent of cybercrimes in the state had originated in LAN house computers.

Several legal provisions, including Article 57-D of the recently revised electoral law, place restrictions on anonymity. Users are generally required to register with their real names before purchasing mobile phones or opening a private internet connection, though the use of pseudonyms in discussion forums is common. There have been no reports of such registration being employed to punish users for their online speech on political or social issues, largely because there are no government efforts to track who participates in such discussions.

While traditional media workers are often victims of violence and death threats in Brazil,[57] such attacks have yet to extend significantly to online journalists, bloggers, and commentators. However, the line between traditional and online journalism is blurred at times, as many reporters straddle the two types of media. In October 2010, radio journalist Francisco Gomes de Medeiros, who reported on organized crime both for radio and on his personal blog, was shot and killed in front of his home by a gunman apparently working for an imprisoned drug trafficker.[58] In 2009 and 2010, there were no widely reported physical attacks solely as retribution for online expression, though some bloggers reported receiving threats of lawsuits.

Cyberattacks plague Brazil, with targets ranging from online banking sites to energy plants.[59] In 2009, several prominent intelligence sources confirmed that a series of

[56] O'Brien, "Is Brazil the Censorship Capital of the Internet? Not Yet."

[57] Maira Magro, "Police Accuse Three Men of Torturing Editor in Northeast Brazil," *Journalism in the Americas*, June 10, 2010, http://knightcenter.utexas.edu/blog/?q=en/node/7449; Maira Magro, "Reporter Who Exposed Death Squad in Brazil Receives Threats," *Journalism in the Americas*, May 25, 2010, http://knightcenter.utexas.edu/blog/?q=en/node/7300; Maira Magro, "Escaped Killer of Brazilian Journalist Turns Himself In," *Journalism in the Americas*, May 25, 2010, http://knightcenter.utexas.edu/blog/?q=en/node/7302.

[58] Danny O'Brien, "Six Stories: Online Journalists Killed in 2010," Committee to Protect Journalists (CPJ), December 17, 2010, http://www.cpj.org/internet/2010/12/online-journalists-killed-in-2010.php.

[59] Dmitry Bestuzhev, "Brazil: A Country Rich in Banking Trojans," Securelist, October 16, 2009, http://www.securelist.com/en/analysis/204792084/Brazil_a_country_rich_in_banking_Trojans.

cyberattacks in January 2005, September 2007, and November 2009 were responsible for blackouts.[60] The blackouts generally occurred at night and were relatively short, causing only limited economic damage. The Brazilian government has denied that the power outages were caused by hacking, but Brazilian hackers have published comments on their blogs affirming that the energy control system is vulnerable to such attacks.[61] An increasing amount of hacker instructional material is produced in Brazil, including information on how to conduct illegal mobile-phone wiretaps or hack passwords.[62]

[60] "Cyber War: Sabotaging the System," *60 Minutes*, CBS, November 8, 2009, http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml; Kevin Poulsen, "Report: Cyber Attacks Caused Power Outages in Brazil," *Wired*, November 7, 2009, http://www.wired.com/threatlevel/2009/11/brazil/.

[61] Apagão Brasil—Mistério ou Ataque Hacker?" [Brazilian Blackout— Mystery or Hacker Attack?], Papituss Log.com, http://www.papitusslog.com/2009/11/apagao-brasil-misterio-ou-ataque-hacker.html.

[62] For examples of tools and hardware for "do-it-yourself wiretapping," see ItecDiffusion.com at http://www.itecdiffusion.com/PT/escuta_telemovel.html; See for example Apostila Hacker [Hacker Toolkit], at http://www.apostilahacker.com.br/.

BURMA

	2009	2011
INTERNET FREEDOM STATUS	n/a	Not Free
Obstacles to Access	n/a	23
Limits on Content	n/a	29
Violations of User Rights	n/a	36
Total	n/a	88

POPULATION: 53.4 million
INTERNET PENETRATION: 1 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

While the Burmese military junta is interested in expanding and exploiting information and communication technologies (ICTs) for business and propaganda purposes, it makes aggressive attempts to regulate access to the internet and digital media, control content, and punish citizens for any online activity that is seen as detrimental to regime security. The government uses a wide range of means to restrict internet freedom, including legal and regulatory barriers, infrastructural and technical constraints, and coercive measures such as intimidation and lengthy prison sentences. Although the authorities lack the capacity to pervasively enforce all restrictions, the impact of sporadic implementation and the ensuing chilling effect is profound.

There has been gradual improvement in access to ICTs over the past three years, but the junta has also aggressively targeted users who are involved in antigovernment activities or have contact with foreign news media. Since its crackdown on a wave of September 2007 protests led by Buddhist monks, the military regime has more strictly enforced licensing rules that require the owners of cybercafes, where most Burmese users obtain access, to monitor users' screens and cooperate with criminal investigations. Both online and offline censorship and information controls were increased surrounding the November 7, 2010 national elections,[1] which secured a sweeping victory for the military-backed party and were

[1] Ba Kaung, "Junta Starts New Censorship Rules," *Irrawaddy*, June 28, 2010, http://irrawaddy.org/article.php?art_id=18823; Reporters Without Borders, "No Credible Elections Without Media Freedom," news release, March 26, 2010, http://en.rsf.org/burma-no-credible-elections-without-26-03-2010,36847.html.

widely condemned as flawed.[2] Censorship was further reinforced after the release of pro-democracy leader Aung San Suu Kyi from house arrest on November 13.

The state-owned Myanmar Post and Telecommunications (MPT) company launched the first official e-mail service in November 1997. The 2002 establishment of the first private internet-service provider (ISP), Bagan Cybertech, helped to increase the number of users in the country, though the company was later taken over by the junta. By 2010, there were over 520 registered cybercafes in Burma, located mainly in a few major cities.[3] The government's first attempt to restrict internet freedom was the 1996 Myanmar Computer Science Development Law,[4] which made possession of an unregistered computer modem and connection to unauthorized computer networks punishable by up to 15 years in prison.[5] Other laws and actions since then have furthered the government's efforts to clamp down on unsupervised internet use.

OBSTACLES TO ACCESS

Internet access and usage are extremely limited due to government restrictions, lack of infrastructure, and widespread poverty. The number of internet users is difficult to ascertain, as independent surveys are not available, and the government offers little credible reporting on these statistics.[6] According to the International Telecommunication Union, there were 110,000 internet users as of 2009, amounting to 0.2 percent of the population.[7] MPT reports that there are 400,000 internet users in Burma.[8]

The price of a private internet connection is prohibitively expensive in a country where an estimated 32 percent of the population lives below the poverty line,[9] though there is significant regional variation.[10] According to the International Monetary Fund, the gross

[2] "UN envoy: Myanmar must address criticism of polls", November 28, 2010, Associated Press, http://www.salon.com/wires/allwires/2010/11/28/D9JP4BMO0_as_myanmar_un/index.html.

[3] Author's interview with a weekly journal editor who oversees internet-related reporting and asked to remain anonymous, December 29, 2010.

[4] In June 1989, the military junta changed the English rendering of the country's name from Burma to Myanmar. Democracy activists and their foreign supporters, including the U.S. government, have continued using Burma.

[5] Computer Science Development Law, September 20, 1996, Chapter X, available at https://www.myanmarisp.com/ICTnews/law10-96.

[6] Bharat Book Bureau, "Myanmar (Burma)—Telecoms, Mobile & Internet," September 2010, http://www.bharatbook.com/Market-Research-Reports/Myanmar-Burma-Telecoms-Mobile-Internet.html.

[7] International Telecommunication Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#.

[8] "Over 400,000 People Using Internet in Burma" [*Myanmar Naing Ngan Twin Internet Ah Thone Pyuit Thu Lay Thein Kyaw Shi Nay Pi*], Eleven News, July 2010, http://www.news-eleven.com/index.php?option=com_content&view=article&id=4000:2010-07-28-06-40-27&catid=42:2009-11-10-07-36-59&Itemid=112.

[9] World Bank, "Data: Myanmar," http://data.worldbank.org/country/myanmar, accessed September 20, 2010.

[10] For example, Chin State has the highest level of poverty, at more than 70 percent. These figures are likely to be conservative, as they are based on data collected before significant increases in fuel prices in October 2005 and August 2007, and an inflationary public-sector salary hike in April 2006. Charles Petrie, End of Mission Report: UN Resident and Humanitarian

domestic product per capita was US$469 for 2010.[11] By comparison, the installation cost for household broadband access is approximately US$1,500, while the monthly fee for service ranges from US$45 to US$130. Other high-speed internet services recently introduced cost somewhat less (approximately US$900 for installation), but remain beyond the reach of most Burmese.[12] In addition, as part of the process for registering an internet connection, consumers must present their national ID, as well proof of police clearance, and a personal affidavit affirming they are not involved in political activities. Because of such barriers, a majority of users rely on cybercafes, where access typically costs about 300 to 600 kyats (US$0.30 to US$0.60) per hour. The shops usually charge an extra 100 kyats (US$0.10) per hour if a power outage occurs and they must rely on generators, which is very common in Burma due to a general lack of electricity. In some cities, the access price may be 1,000 to 1,500 kyats (US$1 to US$2) per hour. The government pledged to extend ADSL broadband coverage to every township by 2006, but implementation has been limited, with service reaching Pyinmana, adjacent to the new administrative capital of Naypyidaw, only in 2007.[13] In 2008, MPT announced that ADSL service was available in 36 cities across Burma.[14] Despite such expansion, internet access has not grown dramatically in practice because of high price and power shortages.

There were 0.90 mobile-phone subscriptions per 100 inhabitants in 2009,[15] and 1.62 fixed telephone lines per 100 inhabitants.[16] Phones are concentrated in large cities like Rangoon and Mandalay, whereas the vast majority of the population lives in underserved rural areas.[17] In 2010, mobile-phone service using the CDMA standard was introduced in Rangoon, Mandalay, and Naypyidaw at a rate of 500,000 kyats (US$500). Cheaper prepaid GSM mobile SIM cards (US$20) were available beginning in 2009, but the buyer was required to present identification documents, and the seller to retain copies. As many SIM card vendors avoided such regulations, in early November 2010, the authorities ordered an end to the sale of unregistered SIM cards.[18] By late November 2010, such sales had generally ceased, though a $50 CDMA pre-paid card remained on the market at year's end.

Coordinator, UNDP Resident Representative for Myanmar, 2003–2007, April 1, 2008, available at http://www.pyinnya.com/wp-content/uploads/2008/06/end-of-mission-report-by-charles-petrie-april-2008.pdf.

[11] International Monetary Fund, "World Economic Outlook Database," April 2010, http://www.imf.org/external/pubs/ft/weo/2010/01/weodata/index.aspx.

[12] "Fibre-optic net in Yangon 'soon': MPT", *Myanmar Times*, September 6-12, 2010, http://www.mmtimes.com/2010/info/539/tech002.html.

[13] "Pyinmana Hooked In To ADSL" [*Ye Htet and Thein Win Nyo*], *Myanmar Times*, July 1, 2007, http://www.mmtimes.com/no372/n019.htm.

[14] "The Internet in Burma (1998–2009)," Mizzima News, December 24, 2009, http://www.mizzima.com/research/3202-the-internet-in-burma-1998-2009-.html.

[15] ITU, "ICT Statistics 2009—Fixed Telephone Lines," http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#

[16] ITU, "ICT Statistics 2009—Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#.

[17] Telecommunications Research Project, Burma (Myanmar) (Hong Kong: University of Hong Kong, October 2007), http://www.trp.trpc.com.hk/publications/myanmar.pdf

[18] "SIM card sales blocked in Rangoon", Democratic Voice of Burma, November 6, 2010, http://www.dvb.no/elections/sim-card-sales-blocked-in-rangoon/12622.

The government exerts control over the internet infrastructure in two ways: total shutdowns, and temporary reductions in bandwidth to slow the flow of information. During the 2007 street protests, the junta completely shut down internet connectivity from September 29 to October 4. From October 4 to 15, the government introduced a "regulated shutdown," meaning connectivity was available only on one ISP, or during late-night curfew hours.[19] According to ICT experts in Burma, the state-controlled ISPs occasionally apply bandwidth caps to prevent the sharing of video and image files,[20] particularly during politically sensitive events, or whenever the junta perceives a risk of damaging information flowing out of the country. For instance, the junta has disabled the mobile-phone network in areas where protests or bomb blasts have taken place.[21] Most recently, internet connections met with interruption between late October and the end of December 2010, surrounding the November elections. Users found networks running at a slow speed and intermittently being completely unavailable. During the week prior to the polls and on election day itself, users reported being completely unable to upload image or video files. In provincial areas, connectivity was worse than in Rangoon.[22] The Myanmar teleport attributed some of the interference to external cyber attacks.[23]

The junta sporadically blocks access to Yahoo! Mail, MSN Mail, Gmail, the video-sharing site YouTube, the messaging feature of the social-networking site Facebook, Google's Blogspot, and the microblogging service Twitter.[24] Several users reported difficulties accessing their Gmail accounts in the run-up to the November elections. However, Voice over Internet Protocol (VoIP) systems including Skype are available. The catalysts for blocks on such applications are not always clear, as censorship policies are generally erratic and opaque. In October 2010, the regime launched the Yatanarpon Teleport (YTP) web portal, which was set to offer e-mail and messenger services, a social-networking platform, a blog-hosting application, discussion forums, and online shopping and banking. By attracting users to this system of domestic services, which in many ways resembles a national intranet, the regime apparently aims to reduce reliance on well-known international services such as Yahoo! Mail, Google's Gmail, and various free blog-hosting sites and discussion forums.[25]

[19] OpenNet Initiative, "Pulling the Plug: A Technical Review of the Internet Shutdown in Burma," OpenNet Initiative Bulletin, November 2007, http://opennet.net/research/bulletins/013.

[20] Author's interviews with a weekly journal editor who oversees internet-related reporting and an information-technology engineer working in the private sector, September 23 and 25, 2010.

[21] Author's interview with a local journalist from Rangoon, September 22, 2010.

[22] Author's interview with two cybercafe owners, five regular internet users and three journalists in Rangoon, Mandalay, and Bassein who requested to remain anonymous, December 29, 30, 2010, and January 2 and 3, 2011.

[23] "Myanmar Internet link continues to meet with interruption", Xinhua News, November 3, 2010, http://english.peopledaily.com.cn/90001/90781/90877/7187339.html and "Attacks on Junta-related Sites Slowing Burma's Internet", *The Irrawaddy Online*, December 24, 2010, http://www.irrawaddy.org/highlight.php?art_id=20406.

[24] Author's interview with three cybercafe owners and eight regular internet users in Rangoon, Mandalay, Bassein, Taunggyi, Naypyidaw, and Myitkyina who requested to remain anonymous, July 11, 19, 25, and 28, 2010.

[25] Htet Aung, "Regime Unveils Burma's First National Web Portal," *Irrawaddy*, August 26, 2010, http://www.irrawaddy.org/article.php?art_id=19311&page=1.

Internet regulations ban circumvention methods, and Burmese ISPs block many bypass and proxy websites, but they lack the technology to block circumvention software like Your Freedom, UltraSurf, and Tor. In many cybercafes, the staff can view the screens of customers, allowing them to detect any attempts at circumvention, which they are encouraged by the authorities to do. However, most staff members offer proxy addresses as a way to attract and retain customers.

There are two main internet-service providers in Burma: MPT and Yatanarpon.[26] In December 2007, the government opened the Yatanarpon Cyber City, where YTP is based.[27] The telecommunications hub is reportedly run by a teenage grandson of Senior General Than Shwe, the regime's top leader. According to several recent reports, the government restructured the ISP system in October 2010, dividing it into two main networks: the MPT ISP, and a newly-created Ministry of Defense (MoD) ISP.[28] Under the new arrangement, the Yatanarpon Teleport ISP (serving civilian users) and a newly-established Naypyitaw ISP (serving most government ministries) connect to the international internet via MPT. Meanwhile, the MoD ISP solely serves users from the Ministry of Defense. Such architecture enables the junta to cut off access for civilians, including government employees, at times of political turmoil, while keeping the military's connection intact. According to Reporters Without Borders, the arrangement may also facilitate monitoring of users and hacking of private accounts, as MITM (Man in the Middle) attacks and DNS spoofing can be targeted at the civilian user network without risking security breaches for military accounts.[29]

There are a number of official institutions tasked with ICT development and management, including the Myanmar Computer Science Development Council, the e-National Task Force (e-NTF), the Myanmar Computer Federation (MCF), and three associations—the Myanmar Computer Professionals' Association (MCPA), the Myanmar Computer Industry Association (MCIA), and the Myanmar Computer Enthusiasts' Association (MCEA). However, these entities are not particularly active, or exist only on paper. In practice, the regime uses intelligence agencies and the Information Ministry to implement its generally arbitrary and ad hoc censorship decisions.

---

[26] Nilar Aye, "Current Status of PKI Development in Myanmar," The Workshop on CA-CA Interoperability Framework in ASEAN August 5-6, 2010, http://www.gits.net.th/Documents/CA-CA_Interoperability_ASEAN/CA_Workshop_2_8_10_Myanmar_updated.pdf . Xinhua news, however, noted as "the Myanmar Teleport (previously known an Bagan Cybertech) and Myanmar Posts and Telecommunications", "Myanmar Internet link continues to meet with interruption," November 3, 2010, Xinhua News, http://english.peopledaily.com.cn/90001/90781/90877/7187341.html.

[27] Ye Kaung Myint Maung, "Nation's First Cyber City Takes Shape," *Myanmar Times*, December 24–30, 2007, http://mmtimes.com/no398/n001.htm.

[28] Author's interview with an official at the Information Ministry who asked to remain anonymous, July 27 and December 30, 2010, and Reporters Without Borders, "National Web Portal Development or Repression?" Burma, November 2010, http://en.rsf.org/IMG/pdf/rap_birmanie-2.pdf.

[29] Ibid.

LIMITS ON CONTENT

The government blocks political websites and media sites run by the Burmese exile community that are critical of the regime and its activities. The government attempts to block most sites containing words it considers suspicious, such as "Burma," "drugs," "military government," "democracy," "student movement," "8888" (a reference to the protest movement that began on August, 8, 1988), and "human rights."[30] YTP blocks almost all Burmese exile and foreign Burmese-language media outlets and blogs, as well as the sites of dozens of foreign newspapers and television networks. It also blocks the websites of international human rights groups. Often, sites are temporarily available only to be blocked again later, and the strength of enforcement apparently varies over time and among the ISPs.[31] According to an engineer from MPT's data and communication department, the company receives lists of URLs, updated weekly, from an army major responsible for web censorship. Following Aung San Suu Kyi's release from house arrest in November 2010, the authorities issued orders barring the publication of interviews with her in print or online.[32]

For blogs whose links are not blocked, the regime has been known to intimidate bloggers to remove certain content. For instance, blogger Win Zaw Naing, was ordered by police to remove certain photographs and articles related to the September 2007 protests, although his blog remained accessible in Burma throughout 2008 and 2009.[33] In addition, the Press Scrutiny Board is known to order news outlets to delete from their websites articles that have been barred from publication in their hard copy versions. However, the government does not appear to have issued any instructions for websites to censor the comment sections beneath articles, one of the main spaces in the online sphere where open and critical discussions take place.

In 2009, after several internal documents, photographs, and video material—including footage showing the construction of underground tunnels and a top general's secret trip to North Korea—were leaked to exile news media, the junta prohibited civil servants in key government ministries from using the internet without authorization from a director-level officer.[34] The government also instructed at least two deputy ministers to head inspection teams that have since launched surprise checks for any unauthorized

[30] Bureau of Democracy, Human Rights, and Labor, "Burma," in 2009 Country Reports on Human Rights Practices (Washington, DC: U.S. State Department, March 11, 2010), http://www.state.gov/g/drl/rls/hrrpt/2009/eap/135987.htm.

[31] "Burmese Blogs Blocked Again After Available for Four to Five Days" [*Myanmar Blog Myar Pyi Twin Hmar Lay Ngar Yet Pwint Pi Hma Pyan Pate Soet Khan Ya*], Radio Free Asia, January 6, 2010, http://www.rfa.org/burmese/news/blog_freedom_lasts_few_days_only-01062010115747.html.

[32] "Local Media Barred from Publishing Suu Kyi Interviews", *The Irrawaddy Online*, December 17, 2010, http://www.irrawaddy.org/article.php?art_id=20340.

[33] Reporters Without Borders, "Another Blogger Arrested for Posts about Saffron Revolution," IFEX, November 16, 2009, http://www.ifex.org/burma/2009/11/16/blogger_arrested/.

[34] Aung Thet Wine, "Internet Use Limited in Government Ministries" [*Wongyi Htar Na Myar Twin Internet Thone Swel Hmu Kant Thet*], *Irrawaddy*, September 10, 2009, http://www.bur.irrawaddy.org/index.php/news/1785-2009-09-10-09-25-20.

downloads of government data at ministries in Naypyidaw.[35] All computers at ministry offices have been password protected, and staff members must make official records whenever they use a computer. Applications that are not necessary for work-related activity were removed from the ministries' computers, reportedly leaving many machines as little more than word processors.[36]

The junta also set up a "Blog Supervising Committee" in every government ministry in late 2007, and instructed civil servants to write pro-government blogs to counter outside bloggers and foreign or exile media, and to attack democracy activists like Aung San Suu Kyi with abusive language.[37] Implementation of the initiative has been inconsistent, but as of December 2010, several such pro-junta blogs remained active.

Harsh prison terms and the selective enforcement of laws such as the Electronic Transactions Law encourage self-censorship, which is common among most internet users, although expression in online comment features where posters can remain anonymous is relatively free. Negative reporting about top military leaders and their family members, or about China (for instance, the news of a jailed Chinese dissident winning the Nobel Peace Prize), are particularly sensitive topics on which users routinely exercise self-censorship.[38]

Prior to the September 2007 protest movement, most ordinary bloggers in Burma focused on personal matters and living conditions. After the protests, however, many grew more explicitly political and funneled news and visual content to foreign and exile media.[39] There are now over 10,000 blogs in Burma's blogosphere. According to an October 2010 survey conducted inside Burma by interviewing 5,076 respondents, blogging was the fastest growing aspect of Burmese internet use in 2010, registering a 25 percent increase from 2009.[40] According to another survey conducted by blogger Nyi Lynn Seck in 2009, about 52 percent of Burmese bloggers write from Burma and 48 percent write from abroad. Some 35 percent of bloggers are 26 to 30 years old, and 29 percent are 21 to 25 years old. About 80 percent blog in Burmese, while 8 percent blog in English and 10 percent write in both

[35] "Surprise Inspections Launched at Ministries Due to Information Leaks" [*Thadin Paukkyar Hmu Myar Jhaut Wongyi Htar Na Myar Go Shaung Ta Khin Sit Say*], Radio Free Asia, August 31, 2009, http://www.rfa.org/burmese/news/investigation_teams_formed_for_news_leaks-08312009153614.html.

[36] Confirmed in interview with staff member at the Myanmar Port Authority, December 2010.

[37] "Ministries to Write Blogs as Counteroffensive" [*Blog Phyint Tont Pyan Yan Wongyi Htar Na Myar Ko Tait Tun*], Mizzima News, July 15, 2008, http://www.mizzimaburmese.com/archive/1414-2008-07-15-10-55-17.html. The most prominent pro-government blogs are located at http://kyeesaytaman.blogspot.com/, http://padaukmyay.blogspot.com/, http://tharkinwe.blogspot.com/, and http://myanmartodayblog.blogspot.com/.

[38] The only local news journal to report on the award was the Weekly Eleven which did so under the headline "China Criticizes Norway for Awarding Liu," October 11, 2010, http://news-eleven.com/index.php?option=com_content&view=article&id=5329:2010-10-10-16-34-26&catid=49:asia&Itemid=118. Observers noted that the censors allowed its publication because the report emphasized the negative angle of the story. "Junta Restricts Nobel News," *The Irrawaddy,* October 12, 2010, http://www.irrawaddy.org/article.php?art_id=19709.

[39] Aung Zaw, "The Cyber Dissident," Irrawaddy Magazine 16, no. 3 (March 2008), http://www.irrawaddymedia.com/article.php?art_id=10647.

[40] "Blogging Increases 25% Within A Year" (*Blog Yay Thar Hmu Ta Nhit Ah Twin 25 Yar Khaing Hnoan Toe Lar*), Internet Journal, December 17, 2010, http://myanmarinternetjournal.com/local-news/2647-2010-12-17-04-31-29.

languages. The rest use ethnic minority languages such as Kachin, Karen, and Chin.[41] In addition to blogs focusing on personal issues, politics, and entertainment, a number address religion, technology and the internet, and literature, among other topics. The blogging platforms they use include Blogspot (77 percent), WordPress (20 percent), Xanga, Ning, Tumblr, and others.[42] These platforms are banned in Burma, but the use of proxy servers and other circumvention tools is reportedly common.[43]

Users regularly share information on useful proxies and other technical knowledge, and have organized gatherings, such as BarCamp, with the permission of the regime.[44] As noted above, some cybercafes provide assistance on how to access banned services like Gmail, and they often ignore users who visit exile media sites. There are now 26 computer universities dedicated to professional education in ICT fields, providing another source of technical expertise.

In the run-up to the November 2010 elections, bloggers reportedly held meetings to discuss various ways to bypass the junta's internet restrictions, with some planning to use a group blog to report on election-related developments to make it more difficult for the authorities to trace the source of information.[45] In the aftermath of the elections, local weeklies were barred from covering the views of losing candidates, a gap filled by exile websites and radio stations. In addition, Aung San Suu Kyi's release shortly after the elections generated intense discussions over Twitter, blogs, Facebook, and other social media. Both before and after her release, Suu Kyi expressed her intention to use ICTs and applications like Twitter to connect with the younger generation after years of isolation, and to create what she termed a "people's network" to bring about democratic change; her comments generated considerable interest among the blogging community.[46] Also in 2010, Burma's exile community used ICTs to create a "Citizen of Burma Award" and confer it on a respected movie star–turned–social worker who had founded the Free Funeral Services Society and Hospice despite harassment from the junta. The honoree was selected through an online nomination and voting system.[47]

---

[41] Nyi Lynn Seck, "Myanmar Blogger Survey 2009," (Rangoon: Myanmar Blogger Society, February 2, 2010), slides, http://www.slideshare.net/lynnseck/myanmar-blogger-survey-2009. The survey was conducted in August and September 2009 at http://freeonlinesurveys.com/rendersurvey.asp?sid=9a6oy3au0kgurai625943, and the result was evaluated from 349 valid responses.

[42] Ibid.

[43] Bob Dietz and Shawn W. Crispin, "Media Freedom Stalls as China Sets the Course," Committee to Protect Journalists, February 10, 2009, http://cpj.org/2009/02/media-freedom-china.php.

[44] Tan, "Myanmar's First Barcamp in Yangon," Global Voices, February 2010, http://globalvoicesonline.org/2010/02/01/myanmars-first-barcamp-in-yangon; author's interview with a weekly journal editor who oversees internet-related reporting, September 22, 2010.

[45] Agence France-Presse, "Burma's Netizens Boot Up for Elections," Democratic Voice of Burma, September 1, 2010, http://www.dvb.no/elections/burmas-netizens-boot-up-for-elections/11527; Phoebe Kennedy, "Burma's Junta Can't Escape from the Net," Independent, September 14, 2010, http://www.independent.co.uk/news/world/asia/burmas-junta-cant-escape-from-the-net-2078458.html.

[46] Author's interview with three young bloggers in Rangoon. December 29, 2010 and January 2, 2011.

[47] The Citizen of Burma Award website is located at http://2011.citizenofburma.org/.

VIOLATIONS OF USER RIGHTS

The military junta ruled the country without a constitution for two decades after 1988, when it took power in a coup and crushed a prodemocracy uprising. The new constitution, drafted by the junta and approved in a flawed 2008 referendum, does not guarantee internet freedom. It simply states that every citizen may exercise the rights "to express and publish their convictions and opinions" if they are "not contrary to the laws, enacted for Union security, prevalence of law and order, community peace and tranquility, or public order and morality."[48] The regime has promulgated three laws regarding ICTs: the Computer Science Development Law (1996), the Wide Area Network Order (2002), and the Electronic Transactions Law (2004).[49] The Printers and Publishers Registration Act (1962) is used to censor the media. All of this legislation and related regulations are broadly worded and open to arbitrary or selective interpretation and enforcement, generating a climate of fear.

In April 2010, an official from the government's Cyber Crime Department reportedly warned that the state would impose harsh punishment for any online activities related to politics.[50] Under Section 33 of the Electronic Transactions Law, internet users face prison terms of 7 to 15 years, and possible fines for "any act detrimental to"—and specifically "receiving or sending and distributing any information relating to"—state security, law and order, community peace and tranquility, national solidarity, the national economy, or national culture.[51] The Television and Video Law (1996) penalizes anyone who possesses a television set, satellite dish, or videocassette recorder and who uses such technology to copy, distribute, sell, or exhibit video recordings without authorization from the state censorship board. Violators face three years in prison or a heavy fine.[52]

The junta makes judicial appointments and interferes with the decisions of judges. Trials for bloggers and other online activists are grossly unfair, lacking due process and typically held in special closed courts. Most defendants are denied access to legal counsel or adequate time to prepare a defense.[53] Like other political prisoners in Burma, individuals

[48] A copy of the constitution in English is available at http://burmadigest.info/wp-content/uploads/2008/11/myanmar_constitution-2008-en.pdf.

[49] Burma Lawyers' Council, "Myanmar Law (1988–2004)," http://www.blc-burma.org/html/Myanmar%20Law/Indexs/lr_law_ml_index.html.

[50] Nayi Lin Latt, "Cyber Hum Khinn Thadin Pha-lel Yay Toe Myint Si Sin" [Increased Information Exchange on Cyber Crimes], Irrawaddy, April 9, 2010, http://www.irrawaddy.org/bur/index.php/news/1-news/2984-2010-04-09-07-29-14.

[51] Electronic Transactions Law, State Peace and Development Council Law No. 5/2004, available at http://www.blc-burma.org/html/myanmar%20law/lr_e_ml04_05.htm.

[52] Television and Video Law, State Law and Order Restoration Council Law No. 8/96, available at http://www.blc-burma.org/html/myanmar%20law/lr_e_ml96_08.html.

[53] Amnesty International, "Myanmar Submission to the UN Universal Periodic Review Tenth session of the UPR Working Group of the Human Rights Council: January 2011," http://www.amnesty.org/en/library/asset/ASA16/008/2010/en/c0d0b33c-31ec-4cfe-b38a-ebae72909704/asa160082010en.html.

detained on internet-related charges are at risk of torture and medical neglect in custody. Lawyers who take on free expression cases have themselves faced punishment. In late October and early November 2008, two defense lawyers, Nyi Nyi Htwe and Khin Maung Shein, were imprisoned for six and four months, respectively, for contempt of court after taking seemingly innocuous actions on behalf of their clients. Four more defense lawyers—Kyaw Hoe, Maung Maung Latt, Myint Thaung, and Khin Htay Kyew—were barred from representing their clients, including members of the 88 Generation Students group, who were charged under the Electronic Transactions Law and other statutes for their use of the internet and "unlawful" e-mail correspondence.[54]

According to Amnesty International, the number of political prisoners as of March 2010 was over 2,200,[55] an increase of nearly 80 percent from the period before the 2007 protests. Many of these prisoners—including monks, student activists, bloggers, and online journalists—were charged under ICT-related laws, and sentenced to lengthy prison terms, with some ordered to spend decades behind bars.[56] Sentences for individuals contributing articles or images to exile media are particularly harsh. In 2010, Reporters Without Borders counted at least 15 journalists and two internet activists in detention.[57] One of the latter was Nay Phone Latt, a blogger and owner of three cybercafes, who was sentenced to 20 years and six months in prison in November 2008 for posting a cartoon of Than Shwe on his blog. The proceedings were held in a closed court, the defendant's mother was not allowed to attend the trial, and he was not represented by his defense lawyer, Aung Thein, who had received a four-month jail term for contempt of court.[58]

Blogger Win Zaw Naing, whose arrest was reported in November 2009 after he had been in detention for several weeks, faced up to 15 years in prison for posting pictures and reports about the September 2007 protests.[59] No news of his sentencing was available as of December 2010. In September 2009, freelance reporter Hla Hla Win was arrested and ultimately given a 27-year prison term, including 20 years for violating the Electronic Transactions Law. She worked for the exile broadcast station Democratic Voice of Burma,

[54] Ibid.; see also Asian Human Rights Commission, "BURMA: Two Rights Lawyers Imprisoned for Contempt of Court," news release, November 8, 2008, http://www.ahrchk.net/statements/mainfile.php/2006statements/1761/.

[55] Amnesty International, "Myanmar Opposition Must Be Free To Fight Elections," news release, March 10, 2010, http://www.amnesty.org/en/for-media/press-releases/myanmar-opposition-must-be-free-fight-elections-2010-03-10.

[56] Assistance Association for Political Prisoners (Burma) and United States Campaign for Burma, The Future in the Dark: The Massive Increase in Burma's Political Prisoners, September 2008 (Mae Sot, Thailand: Assistance Assocation for Political Prisoners [Burma]; Washington, DC: United States Campaign for Burma, October 2008), http://www.aappb.org/the_future_in_the_dark_AAPP_USCB.pdf; Human Rights Watch, "Burma: Surge in Political Prisoners," news release, September 16, 2009, http://www.hrw.org/en/node/85614.

[57] Reporters Without Borders, "Press Freedom Barometer 2010: Burma," http://en.rsf.org/report-burma,53.html.

[58] "Burma Blogger Jailed for 20 Years," British Broadcasting Corporation (BBC), November 11, 2008, http://news.bbc.co.uk/2/hi/asia-pacific/7721271.stm.

[59] Reporters Without Borders, "Another Blogger Arrested for Posts about Saffron Revolution," IFEX, November 16, 2009, http://www.ifex.org/burma/2009/11/16/blogger_arrested/.

recording video interviews in Burma and sending them to the Norway-based outlet mostly via the internet. Her associate, Myint Naing, received a total of 32 years in prison.[60]

In January 2010, a former military officer and a foreign affairs official were sentenced to death, and another foreign affairs official was sentenced to 15 years in prison, for the leak, mentioned above, of information and photographs about military tunnels and a general's trip to North Korea. As of December 2010, the executions had not been carried out.[61] Also in January 2010, journalist Ngwe Soe Lin was sentenced to 13 years in prison for working for an exile media outlet. He had been arrested in a cybercafe in Rangoon in June 2009.[62] In July 2010, activist Than Myint Aung received a 10-year prison sentence for violating Section 33(a) of the Electronic Transactions Law by using the internet to disseminate information that was "detrimental to the security of the state." This came on top of a two-year jail term and a three-year jail term for violations of Section 17(1) of the Unlawful Association Act and Section 13(a) of the Immigration (Emergency Provisions) Act, respectively.[63] Most recently, in late December 2010, photographer Sithu Zeya was sentenced to eight years in prison for taking pictures in the aftermath of an April 2010 bomb blast in Rangoon, and for his affiliation with an exiled media outlet.[64]

The record of harsh punishments against critical internet users has fostered self-censorship and an impression of pervasive surveillance. In reality, however, surveillance is generally spotty due to the limited competence or capacity of the authorities, and corruption on the part of local officials. In many criminal cases, including the trials of members of the 88 Generation Students group and of comedian and blogger Zarganar, the military has used materials such as online chat records and e-mail messages as evidence in court. The authorities either monitor internet activity before arrest, or abuse detainees during interrogation to obtain their passwords and electronic documents.

---

[60] Myint Maung, "Appeal Case for DVB Reporter Hla Hla Win," Mizzima News, March 24, 2010, http://www.mizzima.com/news/breaking-and-news-brief/3718-appeal-case-for-dvb-reporter-hla-hla-win.html; see also Committee to Protect Journalists, "Burmese Journalist Handed 20-Year Prison Sentence," news release, January 7, 2010, http://cpj.org/2010/01/burmese-journalist-handed-20-year-prison-sentence.php; Reporters Without Borders, "Appalling 20-Year Jail Sentence for Democratic Voice of Burma Video Reporter," news release, January 5, 2010, http://en.rsf.org/burma-appalling-20-year-jail-sentence-05-01-2010,35833.html.

[61] "Two Receive Death Sentence for Information Leak," Irrawaddy, January 7, 2010, http://www.irrawaddy.org/article.php?art_id=17542; "Burmese Whistle-Blowers Sentenced to Death—BBC Source," BBC, January 7, 2010, http://news.bbc.co.uk/2/hi/asia-pacific/8446462.stm; "Burma to Execute Two Over Secret Tunnels Leak," Times (London), January 8, 2010, http://www.timesonline.co.uk/tol/news/world/asia/article6980654.ece.

[62] Reporters Without Borders, "Another Video Reporter Gets Long Jail Sentence," news release, January 29, 2010, http://en.rsf.org/burma-another-video-reporter-gets-long-29-01-2010,36245.

[63] "Ko Than Myint Aung Ko Naught Htet Htaung Sel Hnit Cha Hmat" [Ko Than Myint Aung Sentenced to Additional 10 Years], Radio Free Asia, July 15, 2010, http://www.rfa.org/burmese/news/accused_bomber_got_10_year_sentence-07152010170049.html; Myint Maung, "Court Extends Prison Sentence of NLD Liberated Area Member," Mizzima News, July 16, 2010, http://www.mizzima.com/news/inside-burma/4122-court-extends-prison-sentence-of-nld-liberated-area-member.html.

[64] Reporters Without Borders, "Photographer Sentenced to Eight Years in Prison," news release, December 28, 2010, http://en.rsf.org/birmanie-photographer-sentenced-to-eight-28-12-2010,39163.html.

Cybercafe owners are required by law to keep records on their customers' activities, and police have free access to them upon request.[65] Many owners do not systematically enforce monitoring of their users, however, often assisting them in circumventing censorship instead. In an effort to close these gaps, since May 2010, the government has increased surprise inspections of cybercafes in Rangoon and instructed owners to post signs warning users not to visit political or pornographic websites.[66] In November 2010, the authorities also instructed cybercafes to install CCTV cameras and assign at least four security staff to monitor users.[67]

In addition to registering their identity when purchasing a mobile phone, individuals are required to register their computers with MPT and obtain the company's permission to create a webpage.[68] These measures are selectively enforced, with authorities especially targeting those suspected of engaging in political activism or transmitting information to exile or foreign media outlets.

The junta is believed to attack opposition websites based abroad. From May to July 2010, the popular site Photayokeking.org, edited by a Burmese army deserter, was hacked, leaving it inaccessible and inoperative. Many leading exile websites—including the Irrawaddy, Mizzima, Democratic Voice of Burma, and New Era Journal—have been temporarily shut down by hackers since 2008.[69] All of the attacks to date have been distributed denial-of-service (DDoS) attacks. Military sources inside Burma say that the junta has dispatched officers to Singapore, Russia, and North Korea for information-technology training, and that these officers are assigned to monitor e-mail messages and telephone conversations, and to hack opposition websites.[70] China also provides training and assistance, according to the Committee to Protect Journalists. The Irrawaddy, based in Thailand, and the Democratic Voice of Burma claim to have traced cyberattacks to addresses in China and Russia, though they could not identify the culprits.[71]

---

[65] Author's interview with cybercafe owners in Rangoon, Mandalay, and Pegu who asked to remain anonymous, July 11 and 28, 2010.

[66] "More Restrictions and Hurdles on Internet Use" [*Internet Ah Thone Py Hmu Ah Paw Khant Thet Hmu Nae Ah Khet Ah Khe Tway Po Myar Lar*], Voice of America, May 3, 2010, https://www.myanmarisp.com/2010/CICT/ict0201/; author's interview, July 6, 2010.

[67] "Myanmar tightens security measures with cybercafe running", Xinhua News, December 1, 2010, http://news.xinhuanet.com/english2010/world/2010-12/01/c_13630683.htm.

[68] OpenNet Initiative, "Country Profiles: Burma (Myanmar)," May 10, 2007, http://opennet.net/research/profiles/burma.

[69] Alex Ellgee, "Another Opposition Website Shut Down by Hackers," *Irrawaddy*, June 19, 2010, http://www.irrawaddy.org/article.php?art_id=18759.

[70] Author's interviews with military officers who joined training in Russia and a former military intelligence officer, July 6 and 25, 2010.

[71] Dietz and Crispin, "Media Freedom Stalls as China Sets the Course"; Committee to Protect Journalists, February 10, 2009, http://cpj.org/2009/02/media-freedom-china.php; Reporters Without Borders, "No Credible Elections Without Media Freedom," March 26, 2010, http://en.rsf.org/burma-no-credible-elections-without-26-03-2010,36847 and "Majority of Cyber Attacks Came from Chinese IP Addresses," *Irrawaddy*, September 28, 2010, http://www.irrawaddy.org/article.php?art_id=19572.

CHINA

	2009	2011
INTERNET FREEDOM STATUS	Not Free	Not Free
Obstacles to Access	19	19
Limits on Content	26	28
Violations of User Rights	34	36
Total	79	83

POPULATION: 1.3 billion
INTERNET PENETRATION: 33 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Although China is home to the world's largest population of internet users, many of whom have shown increasing creativity in pushing back against censorship, the country's internet environment remains one of the world's most restrictive. This reflects the Chinese Communist Party's paradoxical "two-hand strategy" for managing digital technologies: promoting access for the purposes of economic advancement on the one hand, while attempting to secure control over content, especially political communication, on the other.[1] The Chinese authorities thus maintain a sophisticated and multilayered system for censoring, monitoring, and manipulating activities on the internet and mobile phones. This system has been enhanced, institutionalized, and decentralized in recent years, while the ability of citizens to communicate anonymously has been further constrained. Rights campaigners and some ordinary users continue to face prison time for their internet-related activities. Taken together, these controls have contributed to the Chinese internet increasingly resembling an intranet. Many average users, isolated from international social media platforms and primarily exposed to a manipulated online information landscape, may have limited knowledge of key events related to their own country, even when these make headlines around the world.

The Chinese public was first granted access to the internet in 1996, and the number of users has grown exponentially, from 20 million in 2001 to over 400 million[2] in 2010.

[1] Lena L. Zhang, "Behind the 'Great Firewall': Decoding China's Internet media policies from the inside," *The International Journal of Research into New Media Technologies*, Volume 12(3), 2006, 271-291.
[2] Tang Liang, "Guan Zhu Bo Ke De Zhen Mian Ying Dao Zuo Yong" [Pay Attention to the Positive Effect of Blogging], *CNNIC*, July 22, 2010, http://research.cnnic.cn/html/1279785162d2372.html (in Chinese).

Since it was first introduced, however, the ruling Chinese Communist Party (CCP) has consistently sought to assert its authority over the new medium. The underlying system of infrastructural control and filtering technology has been more or less complete since 2003,[3] while more sophisticated forms of censorship and manipulation—particularly those targeting user-generated content—have gained prominence only recently. Nevertheless, due to the egalitarian nature and technical flexibility of the internet, the online environment remains freer and Chinese citizens more empowered than what is possible in the traditional media sector. The country's growing community of bloggers, online commentators, and human rights defenders has played an increasingly prominent role in uncovering official corruption, exposing rights abuses, and mobilizing citizens to protest against censorship itself.

OBSTACLES TO ACCESS

While the role and presence of information and communication technologies (ICTs) has continued to grow rapidly in recent years, users still face key obstacles to full and free access. These include centralized control over international gateways, more permanent blocks on international applications like the Facebook social-networking site and the Twitter microblogging service, and a complete shutdown of internet access in the western region of Xinjiang for several months in 2009 and 2010.

The government-linked China Internet Network Information Center (CNNIC) reported in December 2010 that there were a total of 446 million users in the country (this number is an estimation based on previous annual surveys), an increase of over 126 million since the end of 2008.[4] Given the country's large population and uneven pattern of economic development, however, the overall penetration rate remains just 33.4 percent, slightly higher than the global average.[5] Moreover, the average penetration rate in urban areas (72.6 percent) is over 40 points higher than that in rural areas (27.4 percent); in 2007, the gap was approximately 20 percentage points, suggesting a widening divide.[6] While most users access the internet from home or work, an estimated 33.6 percent use cybercafes.[7] The vast majority of internet connections are via broadband rather than dial-up,[8] although

[3] Zhang Jing, "Wang Luo Shen Cha Xi Tong Yan Zhi Chen Gong, Fan Dong Xin Xi Zi Dong Guo Lv" [Internet Monitor System Auto-Filters Reactionary Messages], (*Jing Hua Daily,* February 26, 2003, http://www.people.com.cn/GB/it/53/142/20030226/931430.html (in Chinese).

[4] CNNIC, *Information and Updates on the Development of the Internet in China, Issue 61 (Beijing: CNNIC, 2010),* http://research.cnnic.cn/img/h000/h12/attach201012061454440.pdf (in Chinese).

[5] Ibid.

[6] CNNIC, *2009 Report on the Development of the Internet in Rural Areas* (Beijing: CNNIC, 2010), http://www.cnnic.cn/html/Dir/2010/04/15/5810.htm (in Chinese).

[7] CNNIC, *The 26th Report on the Development of the Internet in China* (Beijing: CNNIC, 2010), 22.

[8] CNNIC, *The 26th Report on the Development of the Internet in China*, 11.

access to international websites may be slow due to the burden placed on speed by the nationwide content filtering and monitoring system.[9] Use of mobile phones has also spread quickly. According to the Ministry of Industry and Information Technology (MIIT), there were 850.3 million mobile-phone users in China by November 2010, giving the country a penetration rate of over 62.5 percent and the world's largest population of mobile users.[10] Access to the internet via mobile phones is rapidly gaining popularity. By June 2010, 277 million people used this service, more than double the figure from the previous year.[11] All of these trends may be attributed in part to a gradual decrease in the cost of access and concerted government efforts to connect each township.

There is widespread access to internet technology and applications, such as video-sharing websites, social-networking tools, and e-mail services, but extensive restrictions remain in place, particularly on systems whose providers are based outside the country. Applications such as YouTube, Facebook, and Twitter, and international blog-hosting services like WordPress and Blogspot, have been sporadically blocked in the periods surrounding politically sensitive events in recent years. However, since being cut off during the 20th anniversary of the June 4, 1989, military crackdown on the Tiananmen Square protest movement, they have remained blocked most of the time in China.[12] Chinese equivalents—such as Kaixin001.com, Xiaonei.com, Tudou.com, and Youku.com—have emerged and attracted millions of users, but they are more susceptible to government control, and in 2009 some were also inaccessible surrounding sensitive dates.[13] In the days ahead of June 4, 2009, applications including the microblogging platform Fanfou and the file-sharing platform VeryCD were put out of commission due to "technical maintenance."[14] In December 2010, MIIT issued new regulations banning phone calls from computers to land lines, except for those made over the state-owned networks of China Unicom and

[9] James Fallows, "The Connection has been Reset," *The Atlantic,* March 2008, http://www.theatlantic.com/magazine/archive/2008/03/-ldquo-the-connection-has-been-reset-rdquo/6650/.
[10] MIIT, "*April 2010 Informational Technology Industry Monthly Report, [2010 Nian 11 Yue Tong Xin Ye Yun Xing Zhuang Kuang],*" December 21, 2010, http://www.miit.gov.cn/n11293472/n11293832/n11294132/n12858447/13542227.html.
[11] CNNIC, *The 26th Report on the Development of the Internet in China*, 12.
[12] Tania Branigan, "Internet Censorship in China," *Guardian*, January 14, 2010, http://www.guardian.co.uk/world/2010/jan/14/internet-censorship-china; Rebecca MacKinnon, "China Blocks Twitter, Flickr, Bing, Hotmail, Windows Live, etc. Ahead of Tiananmen 20th Anniversary," *CircleID*, June 2, 2009, http://www.circleid.com/posts/20090602_china_blocks_twitter_flickr_bing_hotmail_windows_live/; Google, "Mainland China Service Availability," http://www.google.com/prc/report.html#hl=en, accessed July 22, 2010, Michael Wines and Andrew Jacobs, "To Shut Off Tiananmen Talk, China Disrupts Sites," *New York Times*, June 2, 2009, http://www.nytimes.com/2009/06/03/world/asia/03china.html.
[13] Tien Lo, "Guang Dian Zong Ju: Shi Ping Wang Zhan Guo You Hua Jin Zhen Due Xin Sheng Qi Ye" [State Administration of Radio Film and Television: Only New Privately-Owned Audiovisual Websites Will Be Nationalized], *Beijing Business Today,* February 5, 2008, http://tech.163.com/08/0205/02/43TG2FVB000915BF.html (in Chinese).
[14] Alice Xin Liu, "Chinese Websites 'Under Maintenance,'" *Danwei*, June 3, 2009, http://www.danwei.org/net_nanny_follies/chinese_websites_under_mainten.php; Sky Canaves, "Closed for Business: More Chinese Web Sites," *China Real Time Report*, June 3, 2009, http://blogs.wsj.com/chinarealtime/2009/06/03/closed-for-business-more-chinese-web-sites/.

China Telecom. This fueled speculation that Skype could be blocked, though its Chinese partner TOM Online claimed that the company was continuing to operate as usual.[15]

In some instances, the government has shut down access to entire communications systems in response to specific events. The most dramatic such incident occurred in Xinjiang in the latter half of 2009. In July, following ethnic violence in the region's capital, Urumqi, the authorities initiated a complete shutdown of internet services and restrictions on international calls and mobile-phone access. The move was part of a broader strategy aimed at preventing the spread of unofficial accounts of events in the region; [16] normal access was not restored until May 2010.[17]

Managers of sophisticated circumvention tools like Freegate and TOR reported greater government efforts to block access to them in June and September 2009. Also targeted for blocking were previously available free virtual private network (VPN) providers like Blacklogic.[18]

Internet access service, once monopolized by China Telecom, has been liberalized and decentralized, and users can now choose from among scores of private internet-service providers (ISPs). The government has been willing to liberalize the ISP market in part because of the centralization of the country's connection to the international internet, which is controlled by six to eight state-run operators that maintain advanced international gateways in Beijing, Shanghai, and Guangzhou.[19] This arrangement remains the primary infrastructural limitation on open internet access in the country, as all ISPs must subscribe via the gateway operators and obtain a license from the MIIT. The system essentially creates a national intranet and gives the authorities the ability to cut off any cross-border information requests that are deemed undesirable. Mobile-phone communication is dominated by three state-owned operators: China Mobile, China Telecom, and China Unicom. Under the oversight of the MIIT, connection to the internet via mobile phones is also monitored by the international gateway operators.

The authorities have sought to exercise fairly tight control over the cybercafe business. The issuance of cybercafe licenses is managed by the Ministry of Culture and its local departments, although to obtain a license, a proprietor typically must also

[15] Malcolm Moore, "China Makes Skype Illegal," *The Telegraph*, December 30, 2010, http://www.telegraph.co.uk/technology/internet/8231444/China-makes-Skype-illegal.html.

[16] Michael Wines, "In Latest Upheaval, China Applies New Strategies to Control Flow of Information," *New York Times*, July 6, 2009, http://www.nytimes.com/2009/07/07/world/asia/07beijing.html; Rebecca MacKinnon, "Google and Internet Control in China" (testimony, U.S. Congressional-Executive Commission on China, Washington, DC, March 24, 2010), http://www.cecc.gov/pages/hearings/2010/20100324/mackinnonTestimony.pdf.

[17] Chris Hogg, "China Restores Xinjiang Internet," British Broadcasting Corporation (BBC), May 14, 2010, http://news.bbc.co.uk/2/hi/asia-pacific/8682145.stm.

[18] Owen Fletcher, "China Clamps Down on Internet Ahead of 60th Anniversary," *PCWorld*, September 25, 2009, http://www.pcworld.com/article/172627/china_clamps_down_on_internet_ahead_of_60th_anniversary.html.

[19] CNNIC, "Zhong Guo Hu Lian Wang Luo Fa Zhan Zhuang Kuang Tong Ji Diao Cha" [Statistical Reports on the Internet Development in China], list of documents: http://www.cnnic.cn/index/0E/00/11/index.htm (in Chinese); Actual document used: http://www.cnnic.cn/uploadfiles/doc/2009/1/13/92209.doc, accessed March 23, 2009.

communicate with the Public Security Bureau, State Administration for Industry and Commerce, and other state entities.[20] Beginning in March 2007, the Ministry of Culture indefinitely suspended the issuance of new licenses. However, reports in early 2009 indicated that a limited number of licenses for new cafes would be granted in some cities, such as Chongqing in Sichuan, Nanjing in Jiangsu, and Zengzhou in Henan.[21] In Guangdong province, several licenses were reportedly issued, though these were primarily to cafes that are part of national chains, which are perceived by the government as easier to control than individual businesses.[22]

LIMITS ON CONTENT

The Chinese authorities continue to employ the most elaborate system for internet content control in the world. Government agencies and private companies together employ hundreds of thousands of people to monitor, censor, and manipulate online content. In an indication of the scale of efforts to control online content, according to a top Chinese official, throughout 2010, some 60,000 websites containing "harmful materials" were forcibly shut down, and an estimated 350 million articles, photographs, and videos were deleted.[23] In recent years, additional layers have been added to this apparatus, particularly as the CCP seeks to restrict the use of social-networking and similar applications for political mobilization. Even this heavily censored and manipulated online environment, however, provides more space for average citizens to express themselves and air their grievances against the state than any other medium in China.

The CCP's content-control strategy consists of three primary techniques: automated technical filtering, forced self-censorship by service providers, and proactive manipulation. The purported goal is to limit the spread of pornography, gambling, and other harmful practices, but web content related to sensitive political or social topics is usually targeted at

[20] "Yi Kan Jiu Mingbai Quan Cheng Tu Jie Wang Ba Pai Zhao Shen Qing Liu Cheng" [A look at an illustration of the whole course of the cybercafe license application process], Zol.com, http://detail.zol.com.cn/picture_index_100/index997401.shtml (in Chinese).

[21] Jason Deng, "Wang Ba Pai Zhao Shen Pi Jie Dong" [Suspension of Cybercafe Licenses Lifted], *QQ News*, March 13, 2009, http://tech.qq.com/a/20090313/000392.htm (in Chinese); "Wang Ba Pai Zhao Kai Jin, Jing Ji Han Dong Zhong De Yi Ba Huo" [Suspension of Cybercafe Licenses Lifted: Positive Effect of Economic Recession], *Tien Xia Wang Meng,* December 23, 2008, http://www.netbarcn.net/Html/HotTopics/12231117335286.html (in Chinese); "Zengzhou 2009 Nian Wang Ba Pai Zhao Jiang Shi Du Fang Kai Shen Pi" [Zengzhou Cybercafe License Ban to Be Lifted in Moderation in 2009],*) Henan News Daily*, February 23, 2009, http://www.netbarcn.net/Html/todaynetbar/02232050122415.html (in Chinese).

[22] "Quan Guo Ge Di Guan Yu Wang Ba Pai Zhao Jie Jin De Xing Wen Hui Zong" [Cybercafe Licensing Ban Lifted Across the Country – News Summary], Tien Xia Wang Meng, December 23, 2008, http://www.netbarcn.net/Html/PolicyDynamic/12231119046113.html (in Chinese); "Wang Ba Shen Pi Bing Dong 7 Nian Jie Jin" [Seven-year Freeze on Internet Cafe Licenses Lifeted], *[*Wangba.net, January 19, 2010, http://www.wangba.net/xinwen/12638974233019.shtml (in Chinese).

[23] "China Shuts Over 60,000 Porn Websites This Year," Reuters, December 30, 2010, http://www.reuters.com/article/idUSTOE6BT01T20101230.

least as forcefully.[24] The most systematically censored topics include criticism of top leaders, independent evaluations of China's rights record, violations of minority rights in Tibet and Xinjiang, the Falun Gong spiritual group, the 1989 Beijing massacre, pro-Taiwanese independence viewpoints, and various dissident initiatives that challenge the regime on a systemic level.[25] These standing taboos are supplemented by regular directives on negative developments such as tainted-food scandals, environmental disasters, and deaths in police custody. Broader politically-oriented terms like "democracy," "human rights," and "freedom of speech" are subject to less extensive censorship.[26]

Blocking access to foreign websites is a key component of technical filtering. In addition, deep-packet inspection technologies employed by the authorities enable the filtering of particular pages within otherwise approved sites if the pages are found to contain blacklisted keywords in the URL path.[27] Filtering by keyword is also implemented in instant-messaging services, such as TOM Skype and QQ, and the necessary software is built into the application upon installation.[28]

A large share of censorship is enforced at the level of state-run news outlets and private companies operating a variety of websites. These entities are required by law to ensure—either automatically or manually—that content banned by party and government censorship orders is not posted or circulated widely. They risk losing their business licenses if they fail to comply, and many companies employ large staffs to carry out this task. A series of documents leaked by an employee of the Baidu search engine in April 2009 highlighted both the breadth of topics censored and the complexity of the system used to identify and remove targeted content.[29] In October 2010, a general manager at Baidu Tie Ba reportedly

[24] Hung Huang, "Censorship in Chinese Media," *Economix*, September 25, 2008, http://economix.blogs.nytimes.com/2008/09/25/censorship-in-chinese-media/.

[25] These include, for instance, the prodemocracy manifesto Charter 08 and the *Nine Commentaries*, a series of editorials analyzing the history of the party and encouraging an end to its rule. See graph, "Inaccessible Sites—Top 100 Google Search Results," from OpenNet Initiative, *Internet Filtering in China in 2004–2005: A Country Study*, available at Select Committee on Foreign Affairs, "Written Evidence Submitted by Sarah Cook, Student at the School of Oriental and African Studies, University of London," House of Commons, Session 2006–07, http://www.publications.parliament.uk/pa/cm200607/cmselect/cmfaff/269/269we08.htm; Nart Villeneuve, *Breaching Trust: An Analysis of Surveillance and Security Practices on China's TOM-Skype Platform* (Toronto: Information Warfare Monitor/ONI Asia, 2008), http://www.nartv.org/mirror/breachingtrust.pdf; Julen Madariaga, "Charter 08: Why It Should Be Called Wang," *Chinayourren*, January 11, 2009, http://chinayouren.com/eng/2009/01/charter-08-why-it-should-be-called-wang/.

[26] Ashley Esarey and Xiao Qiang, "Digital Communication and Political Change in China," *International Journal of Communication*, 5 (2011), 298-319.

[27] Ben Wagner, *Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control'* (Global Voices Advocacy, June 25, 2009), http://advocacy.globalvoicesonline.org/2009/06/25/study-deep-packet-inspection-and-internet-censorship/.

[28] Xiao Qiang, "A List of Censored Words in Chinese Cyberspace," *China Digital Times*, August 30, 2004, http://chinadigitaltimes.net/2004/08/the-words-you-never-see-in-chinese-cyberspace/.

[29] Xiao Qiang, "Baidu's Internal Monitoring and Censorship Document Leaked (1)," *China Digital Times*, April 30, 2009, http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked/; Xiao Qiang, "Baidu's Internal Monitoring and Censorship Document Leaked (2)," *China Digital Times*, April 29, 2009, http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked-2/; Xiao Qiang, "Baidu's

disclosed that staff deleted approximately one million entries per day in the search engine's popular function that enables users to create online forums and communities based on keywords.[30] Foreign corporations have also been required to implement censorship of political content in order to gain access to the Chinese market. In March 2010, Google announced that it would stop censoring its search results and began redirecting mainland users to its uncensored Hong Kong–based search engine after Chinese officials made it clear that "self-censorship is a non-negotiable legal requirement."[31] The authorities responded by blocking results of searches with flagged keywords that were initiated by mainland users on the Hong Kong engine; access to the Gmail e-mail service and other Google services remained intact as of the end of 2010.

Most postings on blogs, comment sections of news items, and bulletin-board system (BBS) discussions that are deemed objectionable are deleted by company staff before they appear to the public. Such efforts are often temporarily reinforced surrounding politically sensitive events. For example, starting in April 2010, a popular BBS based in Shanghai (KDS Life) announced a ban on commenting between midnight and 7 a.m. in order to create a "harmonious online environment" for the Shanghai Expo; it also warned that anyone posting "harmful" content during the Expo would be subject to serious penalties.[32] In other cases, individual blog entries may be deleted after the fact, in most instances within 24 to 48 hours of their posting, or entire blogs may be shut down. In one recent case, the blog of prominent artist and activist Ai Weiwei was shut down in May 2009, following repeated postings that revealed details of children's deaths in the 2008 Sichuan earthquake and aired accusations that they were caused in part by local corruption.[33]

The existing censorship techniques have proven insufficient to completely overcome the flexibility of the technology, the sheer volume of communications, and a sometimes intentional disregard for official directives by nonstate actors. A 2008 study of blog-hosting services revealed that domestic censorship varied widely among different sites.[34] The CCP

Internal Monitoring and Censorship Document Leaked (3)," *China Digital Times*, April 28, 2009, http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked-3/.

[30] "Zhong Guo Hu Lian Wang Xin Xi Guan Zhi, Baidu Tie Ba Ri Shan Tie Bai Wan" [Chinese Internet Censorship: Baidu Deletes Million Posts], Yazhou Zhoukan, November 7, 2010, http://www.yzzk.com/cfm/Content_Archive.cfm?Channel=nt&Path=2212930682/44ntd.cfm (in Chinese).

[31] Ellen Nakashima, Cecilia Kang, and John Pomfret, "Google to Stop Censoring Search Results in China," *Washington Post*, March 23, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/22/AR2010032202041.html.

[32] "Shi Bo Qi Jian Ling Chen 0 Dian – 7 Dian Zhan Ting Fa Tie Ji Hui Tie Gong Gao" [BBS Will Be Down From Midnight to 4 AM During Shanghai EXPO], *KDS Life BBS,* April 28, 2010, http://club.pchome.net/thread_7_73_5352801__.html (in Chinese).

[33] Michael Wines, "China's Impolitic Artist, Still Waiting to Be Silenced," *New York Times*, November 27, 2009, http://www.nytimes.com/2009/11/28/world/asia/28weiwei.html; Simon Elegant, "Ai Weiwei's Blogs Shuttered; He Declines to 'Chat' With Police, Not Politely," *The China Blog*, May 29, 2009, http://china.blogs.time.com/2009/05/29/ai-weiweis-blogs-shuttered-he-declines-to-chat-with-police/.

[34] Rebecca MacKinnon, "China's Censorship 2.0: How Companies Censor Bloggers," *First Monday* 14, no. 2 (February 2, 2009), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089.

and government agencies have taken various actions over the past two years to plug these gaps in the censorship system. They have included the following:

- **Antipornography campaign targeting political and social content.** On January 5, 2009, seven government agencies announced the launch of a nationwide campaign to more strictly enforce online censorship regulations.[35] Ostensibly an effort to purge pornographic material, the campaign was widely seen as a means of tightening control over politically sensitive content.[36] Within days of the announcement, Beijing authorities ordered the closure of the blog-hosting website Bullog.cn, which was popular among political commentators and prodemocracy activists, after the site allegedly failed to comply with instructions to remove large amounts of "harmful information" related to current events.[37] In early February, numerous e-groups and individual accounts related to political and social issues on the popular Douban.com social-networking site were reportedly deleted or closed.[38] Later in the year, the campaign was extended to online content available via mobile phones.[39]
- **Tightened control over audio-visual content.** On March 30, 2009, the State Administration of Radio, Film, and Television issued an edict to tighten the management of online audio-visual content.[40] The regulations included a detailed list of content categories to be deleted, such as videos with "depictions of torture" or "distortions of Chinese culture or history," and those that "hurt the feelings of the public," "disparage" security forces or leaders, or are posted by "netizen reporters."[41] The regulations also required service providers to "improve their program content administration" by hiring "well-qualified service personnel to review and filter content." As part of the implementation of these directives, over 530 audio-visual

[35] A list of 19 prominent companies and websites were identified as having failed to purge undesirable content and heed state censors. They included Google, Baidu, Sina, and Sohu. Chris Buckley, "China Targets Big Websites in Internet Crackdown," Reuters, January 5, 2009, http://uk.reuters.com/article/idUKSP36401920090105?sp=true.
[36] Rebecca MacKinnon, "China's Latest Internet Crackdown," *RConversation*, January 5, 2009, http://rconversation.blogs.com/rconversation/2009/01/chinas-latest-i.html.
[37] "China Closes 91 Websites in Online Crackdown," Reuters, January 11, 2009, http://www.reuters.com/article/idUSTRE5040F120090112; Anita Chang, "Activist Blog Closed Amid China's Porn Sweep," Associated Press, January 9, 2009, http://www.msnbc.msn.com/id/28577927/ns/technology_and_science-tech_and_gadgets/.
[38] Oiwan Lam, "China: E-Group Cleaning at Douban.com," Global Voices Advocacy, February 9, 2009, http://advocacy.globalvoicesonline.org/2009/02/09/china-e-group-cleaning-at-doubancom/.
[39] Juliet Ye, "China's Anti-Porn Campaign Goes Wireless," *China Real Time Report*, December 1, 2009, http://blogs.wsj.com/digits/2009/12/01/chinas-anti-porn-campaign-goes-wireless/.
[40] Oiwan Lam, "China: Tightening Control Over Internet Audio-Visual Content," Global Voices Advocacy, April 1, 2009, http://advocacy.globalvoicesonline.org/2009/04/01/china-tightening-control-over-internet-audio-visual-content/.
[41] Freedom House, "Freedom House Dismayed by New Chinese Internet Restrictions," news release, April 2, 2009, http://www.freedomhouse.org/template.cfm?page=70&release=800.

websites reportedly had their licenses revoked for noncompliance by September 2009.[42]

- **Introduction of Green Dam and Blue Shield software.** In May 2009, the Chinese authorities announced that as of July 1, all computer manufacturers would be required to install Green Dam Youth Escort filtering software on their products,[43] ostensibly to protect youth from "harmful" content. However, tests by both Chinese and international experts revealed that the program would monitor and filter activity related to politics and religion; one file with thousands of banned characters was explicitly named "FalunWord.lib," a reference to the persecuted Falun Gong spiritual group to whom the majority of terms in the library related.[44] Moreover, Green Dam was capable of shutting down whole applications, such as web browsers or word processors, when certain keywords were typed.[45] Green Dam's vulnerabilities to malicious software and incompatibility with other programs were also noted. Activists, lawyers, and ordinary users mobilized quickly to protest the directive. With added pressure from the international business community, foreign governments, and human rights groups, the authorities withdrew the order the day before the July 1 deadline.[46] Installation reportedly continued in schools and cybercafes, though some later removed it because it obstructed other crucial programs.[47] In September 2009, reports emerged of technical filtering being moved from the internet backbone down to ISPs via the installation of a program referred to as Blue Shield/Dam.[48] Though no comprehensive studies have been conducted to date, the apparent impact of these installations has been more systematic automated filtering within China and tighter blocks on circumvention software.[49] In July 2010,

[42] "Shi Wan Zhong Xiao Wang Zhan Han Dong Duan Wang" [Licenses of a Hundred Thousand Websites Revoked during Winter], *Southern Metropolis Weekly*, January 18, 2010, http://www.nbweekly.com/Print/Article/9591_0.shtml (in Chinese).
[43] Oiwan Lam, "China: Green Dam PC Filtering," Global Voices Advocacy, June 8, 2009, http://advocacy.globalvoicesonline.org/2009/06/08/china-green-dam-pc-filtering/; Andrew Jacobs, "China Requires Censorship Software on New PCs," *New York Times*, June 8, 2009, http://www.nytimes.com/2009/06/09/world/asia/09china.html.
[44] Scott Wolchok, Randy Yao, and J. Alex Halderman, "Analysis of the Green Dam Censorware System," Computer Science and Engineering Division, University of Michigan, June 18, 2009, http://www.cse.umich.edu/~jhalderm/pub/gd/. For the contents of the FalunWord.lib file see: http://www.cse.umich.edu/~jhalderm/pub/gd/data/falunword.php.
[45] Hal Roberts, "China Bans the Letter 'F,'" *Watching Technology*, June 12, 2009, http://blogs.law.harvard.edu/hroberts/2009/06/12/china-bans-the-letter-f/.
[46] Ian Paul, "Has China's Green Dam Burst?" *PCWorld*, July 1, 2009, http://www.pcworld.com/article/145302/has_chinas_green_dam_burst.html.
[47] Reuters, "Chinese Schools Quietly Remove Green Dam Filter," *PC Magazine*, September 15, 2009, http://www.pcmag.com/article2/0,2817,2352847,00.asp.
[48] Reporters Without Borders, "Is China Imposing More Powerful Version of Green Dam, Called Blue Shield?" news release, September 18, 2009, http://en.rsf.org/china-is-china-imposing-more-powerful-18-09-2009,34518.html; Oiwan Lam, "China: Blue Dam Activated," Global Voices Advocacy, September 13, 2009, http://advocacy.globalvoicesonline.org/2009/09/13/china-blue-dam-activated/.
[49] Rebecca MacKinnon, "China's Censorship Arms Race Escalates," *RConversation*, September 28, 2009, http://rconversation.blogs.com/rconversation/2009/09/index.html..

six internet security systems functionally similar to Green Dam were forced to be installed on computers in schools, hotels, and cybercafés in Guangdong Province and were reportedly promoted in other provinces including Jiangsu and Hebei.[50] As the censorship is taking place at the network or local level and does not impose requirements on foreign companies, it has not provoked significant domestic or international backlash.

- **More deliberate favoritism toward Chinese brands.** Despite increased privatization and competition, China's economic environment remains dominated by the government. Particularly in the case of large companies, success often depends on close relationships with the CCP and relevant officials. Both Chinese officials and independent analysts have attributed the market dominance of locally-managed internet firms such as Baidu[51] over international brands such as Google at least in part to government favoritism, noting the authorities' interest in promoting Chinese companies that will comply more readily with government-imposed content restrictions than foreign firms.[52] In recent years, this strategy has been applied more deliberately to an expanded set of applications, such as video-sharing, microblogging, and social-networking platforms. The result is a "commercialization of censorship," whereby efficient and obedient filtering becomes a key factor in business competition.

Realizing that they are unable to entirely control online content, and increasingly viewing cyberspace as a field for "ideological struggle,"[53] the Chinese authorities in recent years have also introduced measures to proactively sway public opinion online and amplify the Communist Party's version of events over alternative accounts. This effort has taken a number of forms.

First, online news portals are prohibited from producing their own content and are only authorized to repost information from state-run traditional media.[54]

---

[50] "Lv Ba Bien Shen Tou Tou Juan Tu Chong Lai, Dang Jv Qiang Zhi An Zhuang Jian Kong Ruan Jian" [Green Dam Returns in a Discrete Manner, Authorities Require Mandatory Installation of Monitoring Software], *Radio Free Asia Mandarin*, July 30, 2010, http://www.rfa.org/mandarin/yataibaodao/lb-07302010095804.html (in Chinese).

[51] It should be noted that, although locally-managed, Baidu has some international shareholders as well as Chinese. See: iDataCenter Research Service, "Bai Du Shang Shi Hou de Gu Fen Jie Gou Qing Kuang" [Baidu's shareholder situation after its listing on the market], 2005, http://irs.iresearch.com.cn/Consulting/search_engine/Graph.asp?id=7508 (in Chinese).

[52] Jordan Calinoff, "Where Google Loses," *Foreign Policy*, September 29, 2009, http://www.foreignpolicy.com/articles/2009/09/29/where_google_loses; Translation of speech by Peng Bo, Deputy Chief of the State Council Information Office Internet Affairs Bureau, "The Main Problems Relating to Internet News Propaganda," *China Digital Times,* December 17, 2009, http://chinadigitaltimes.net/2009/12/peng-bo-%E5%BD%AD%E6%B3%A2-%E2%80%9Cthe-main-problems-relating-to-internet-news-propaganda%E2%80%9D/.

[53] Oiwan Lam, "China: The Internet as an Ideology Battlefield," Global Voices Advocacy, January 6, 2010, http://advocacy.globalvoicesonline.org/2010/01/06/china-internet-as-an-ideology-battlefield/.

[54] Interim Provisions on the Administration of Internet Websites Engaged in News Posting Operations (November 1, 2000), excerpts available at http://www.cecc.gov/pages/virtualAcad/exp/explaws.php.

Second, in addition to removal orders, propaganda directives are often accompanied by specific instructions to marginalize or amplify certain content, for instance through its position on a homepage or by relying exclusively on the version of events produced by the official Xinhua news agency. Thus in March 2010, during the annual meeting period of the National People's Congress, one set of leaked guidelines reportedly included instructions that "no negative news [is] allowed on the front pages of newspapers or the headline news sections of websites."[55]

Third, since 2005, paid web commentators known collectively as the 50 Cent Party or Red Vests have been recruited to post progovernment remarks, lead online discussions in accordance with the party line, and report users who have posted offending statements. Some estimates place the number of these commentators at over 250,000.[56] In 2009, this strategy appeared to become both more institutionalized and more decentralized, with commentators trained and used by "government units at all levels."[57] For instance, in January 2010 it was reported that Gansu provincial authorities had decided to establish a cadre of 650 online progovernment commentators;[58] in December 2010, Chongqing's municipal authorities created a Red Microblog platform to spread pro-Communist Party messages;[59] and in the aftermath of the Urumqi violence in Xinxiang, the authorities there enlisted local Communist Youth League members to be online "supervisors."[60]

Fourth, mobile-phone communication is now treated as another medium for spreading party ideology. In 2010, a campaign was launched to encourage the dissemination of progovernment "Red text messages" through economic incentives.[61] It is difficult to gauge the effectiveness of these manipulation efforts. On the one hand, there have been cases in which online public opinion rapidly turned in the government's favor.[62] On the other hand,

[55] "What Chinese Censors Don't Want You to Know," *New York Times*, March 21, 2010, http://www.nytimes.com/2010/03/22/world/asia/22banned.html.
[56] David Bandurski, "China's Guerrilla War for the Web," *Far Eastern Economic Review* (July 2008), http://feer.wsj.com/essays/2008/august/chinas-guerrilla-war-for-the-web.
[57] David Bandurski, "Internet Spin for Stability Enforcers," China Media Project, May 25, 2010, http://cmp.hku.hk/2010/05/25/6112/.
[58] Qian Gang, "How Much Internet Freedom Do Chinese Citizens Have?" China Media Project, January 28, 2010, http://cmp.hku.hk/2010/01/28/4355/.
[59] Malcolm Moore, "China Launches Red Twitter," *Telegraph*, December 15, 2010, http://www.telegraph.co.uk/technology/news/8203593/China-launches-Red-Twitter.html.
[60] Jonathan Ansfield, "China Starts to Lift Region's Web Blackout," *New York Times*, December 30, 2009, http://www.nytimes.com/2009/12/30/world/asia/30xinjiang.html.
[61] Chen Jian, "Zhong Guo Liu Qian Wan Ren Can Yu Zhuan Fa Shou Ji 'Hong Duan Zi'" [Sixty Million People Have Participated in 'Red Text Message' Efforts], *Beijing Ren Min Wang*, March 16, 2010. http://news.163.com/10/0316/21/61UI6BNGM000146BD.html (in Chinese); "Hong Duan Zi Zhi 'Ai Wo Zhong Hua Chuang Ye Guang Dong' Wang Luo Chuang Ye Da Sai - - Mei Li Yang Jiang" [China Telecom: Red Text Message – 'Love in China, Opportunities in Guang Dong' Writing Contest], *Baidu,* August 21, 2008, http://hi.baidu.com/liming10liming/blog/item/24de0a234ea6cbfad6cae224.html (in Chinese).
[62] Michael Bristow, "China's Internet 'Spin Doctors,'" BBC, December 16, 2008, http://news.bbc.co.uk/2/hi/asia-pacific/7783640.stm.

participants in online discussion groups have become increasingly adept at identifying 50 Cent Party members and express a dismissive attitude toward their comments.

Following the October 2010 announcement that jailed democracy advocate Liu Xiaobo had been awarded the Nobel Peace Prize, the Chinese authorities activated the full range of above-mentioned measures to restrict the circulation of unofficial news and commentary related to the award, as well as limit citizens' direct access to Liu's writings. In addition, on October 17, 2010, in an effort to sway domestic public opinion, the state-run *People's Daily* published a commentary framing Liu as a political tool of nefarious Western forces aiming to interfere in China's internal affairs. In December, the empty seat left for Liu during the award ceremony in Oslo became a key censorship target. Phrases such as "empty chair," "empty stool," and "empty table" flooded the Chinese cyberspace for a few hours, but were quickly and consistently deleted by staff at the Sina Weibo microblogging platform, the social-networking website Renren, and other new media applications.[63] In addition, authorities disrupted the internet and mobile-phone connections of dozens of prominent activists and bloggers across China. Such actions appeared aimed, among other things, at inhibiting activists' ability to use channels such as the Twitter microblogging service to spread news of the award within China. Reflecting the pervasiveness of government efforts to quash discussion of the prize, on the day of the ceremony, the most discussed topics on the popular web portal Sina appeared to be the cold weather and flight delays at Beijing's airport.[64] Though some users succeeded in circumventing censorship surrounding the award, official and unofficial accounts indicated that fewer than 15 percent of people in China had heard of Liu.[65]

A variety of national and local government agencies are involved in internet censorship, with some instructions coming from the highest echelons of the Communist Party.[66] While much of this apparatus has remained unchanged, two notable adjustments have taken place since early 2009. First, the CCP's Propaganda Department has sought to exercise greater and more specific control over the decision-making process at entities like the MIIT and the State Council Information Office (SCIO), at times coercing them into

[63] Matthew Campbell and Roger Boyes, "Beijing Wipes Web of Photo of Nobel Peace Prize Winner Liu Xiaobo's Empty Chair," *The Australian*, December 13, 2010, http://www.theaustralian.com.au/news/world/beijing-wipes-web-of-pic-of-nobel-peace-prize-winner-liu-xiaobos-empty-chair/story-e6frg6so-1225969772445; Peter Foster, "Nobel Peace Prize: Beijing Under a Censorship Shroud," *Telegraph*, December 10, 2010, http://www.telegraph.co.uk/news/worldnews/asia/china/8194247/Nobel-peace-prize-Beijing-under-a-censorship-shroud.html.

[64] Andrew Jacobs, "Tirades Against Nobel Aim at Audience in China," *New York Times*, December 10, 2010, https://www.nytimes.com/2010/12/11/world/asia/11china.html?_r=1&ref=asia.

[65] Cara Anna, "Some Chinese Elude Censorship of Nobel Prize News," Associated Press, December 8, 2010, http://abcnews.go.com/Technology/wireStory?id=12340665&page=3; Jacobs, "Tirades Against Nobel Aim at Audience in China."

[66] See, for example, Politburo involvement in planning the response to the Nobel Peace Prize and Politburo member Liu Changchun's orders to state-run firms to stop doing business with Google: Jacobs, "Tirades Against Nobel Aim at Audience in China"; James Glanz and John Markoff, "Vast Hacking by a China Fearful of the Web," *New York Times,* December 4, 2010, http://www.nytimes.com/2010/12/05/world/asia/05wikileaks-china.html?pagewanted=1&_r=3.

actions that are contrary to their own vested interests. Second, in April 2010, the government confirmed that it had created a new entity under the SCIO: Bureau 9, tasked with monitoring and coordinating the authorities' response to user-generated content, particularly on social-networking sites and online forums.[67]

Censorship decisions are largely non-transparent, though some private companies are known to alert readers that content has been removed for unspecified reasons. No avenue exists for appealing censorship decisions. Aware of the comprehensive nature of surveillance and censorship on the internet and mobile-phone text messaging, ordinary users and bloggers engage in extensive self-censorship and often refrain from transmitting sensitive comments.

Despite the government restrictions, the internet has emerged in recent years as a primary source of news and a forum for discussion for many Chinese, particularly among the younger generation. According to a 2008-2009 study by CNNIC, 113 million users were found to update either a blog or personal website on a regular basis.[68] Chinese cyberspace is replete with online auctions, social networks, homemade music videos, a large virtual gaming population, and spirited discussion of some social and political issues.[69] Internet users are also able to hold government and CCP officials to account, though only to a limited extent.[70] Civil society organizations involved in education, health care, and other social and cultural issues that are deemed acceptable by the authorities often have a dynamic online presence.

In several cases in 2009 and 2010, Chinese users were able to challenge official misconduct, organize strikes, and obtain justice for ordinary citizens. In a series of strikes at factories owned by the Japanese automaker Honda, workers used internet chat rooms and text messages to coordinate their actions and share information and videos with workers in other locations.[71] The relationship between investigative journalism and online networks can also be mutually reinforcing, particularly when reporting by local commercial outlets is amplified via the internet, enabling wider exposure of the story. In August 2009, after a local newspaper in Shaanxi ran a short article about lead poisoning among children due to pollution from a nearby smelting plant, the popular internet portal Netease picked up the story, drawing national attention to the incident.[72]

---

[67] Jonathan Ansfield, "China Starts New Bureau to Curb Web," *New York Times*, April 16, 2010, http://www.nytimes.com/2010/04/17/world/asia/17chinaweb.html.

[68] CNNIC, *2008-2009 Report on Chinese Bloggers' Market and Behavioral Studies*, (Beijing: CNNIC 2009), http://research.cnnic.cn/html/1247813014d1063.html (in Chinese).

[69] H. Yu, "Blogging Everyday Life in Chinese Internet Culture," *Asian Studies Review* 31 (2007): 423–33.

[70] J. Lacharite, "Electronic Decentralization in China: A Critical Analysis of Internet filtering Policies in the People's Republic of China," *Australian Journal of Political Science* 37 (2002): 2, 333–46; Guobin Yang, *The Power of the Internet in China: Citizen Activism Online* (New York: Columbia University Press, 2009).

[71] David Barboza and Keith Bradsher, "In China, Labor Movement Enabled by Technology," *New York Times*, June 15, 2010, http://www.nytimes.com/2010/06/17/business/global/17strike.html.

[72] Qian Gang, "Central Party Media 'Grab the Megaphone,'" China Media Project, August 21, 2009, http://cmp.hku.hk/2009/08/21/1709/.

Sina Weibo, a microblogging application, has especially grown in popularity since its launch in 2009. As of October 2010, it reportedly registered 50 million users.[73] It has played an increasingly important role in empowering Chinese citizens. In November 2010, Shanghai residents used microblogging and instant messaging services to pressure the local government to conduct an in-depth investigation into a deadly fire that claimed more than fifty lives.[74] In December 2010, the suspicious death of a village head who had been protesting forced demolitions ignited a wave of public outrage as a graphic image of the man's crushed body under a truck was circulated on China's major web portals.[75] Chinese grassroots activists used Sina Weibo to organize citizen investigation groups[76] and disseminate information regarding the incident.[77] However, due to the local government's control of key informants, the results of the citizen investigation appeared less independent than many had hoped.[78]

As controls have tightened in recent years, a growing number of individuals are reportedly seeking out knowledge and techniques for circumventing censorship. In some cases, their specific aim is to join Twitter, which is blocked in China. An activist community of some 30,000 to 50,000 people within China, mostly living in urban areas like Beijing, Shanghai, and Guangzhou, use the tool to rapidly transmit news, connect with other socially conscious individuals, and take advantage of an uncensored medium.[79] Other methods for getting around censorship include using witty alternatives and homonyms for banned keywords, opening multiple blogs on different hosting sites, and using peer-to-peer technologies to circulate banned information. It has become increasingly common for users—including those who would not normally consider themselves politically active—to criticize censorship itself. Throughout the first half of 2009, for example, internet users widely circulated cartoons and videos of a mythical "grass-mud horse" and its struggle

[73] Austin Ramzy, "Wired Up," *Time Magazine*, February 21, 2011, http://www.time.com/time/magazine/article/0,9171,2048171-2,00.html.
[74] Jeremy Page, "Thousands Mourn Fire Victims in Shanghai," *Wall Street Journal,* November 21, 2010, http://online.wsj.com/article/SB10001424052748704444304575628360108943100.html; Oiwan Lam, "China: Messages Behind the Flowers to the Shanghai Fire Victims," Global Voices, November 22, 2010, http://globalvoicesonline.org/2010/11/22/china-messages-behind-the-flowers-to-the-shanghai-fire-victims/.
[75] Xiyun Yang and Edward Wong, "Suspicious Death Ignites Fury in China," *New York Times,* December 28, 2010, http://www.nytimes.com/2010/12/29/world/asia/29china.html.
[76] "Netizens form Groups to Conduct Independent Investigation into Qian Yun Hui Incident [*Wang You Zu Tuan Du Li Diao Cha Qian Yunhui Shi Jian*]," Dong Nan Morning Daily, January 1, 2011, http://news.163.com/11/0101/09/6PA8AFDJ00014AED.html.
[77] "Citizen Alliance Qian Yun Hui Investigation Report [*Gong Meng "Qian Yunhui Zhi Si Zhen Xiang" Diao Cha Bao Gao*]," blog post, Xushiyong Blog, December 31, 2010, http://xuzhiyong.fyfz.cn/art/874568.htm.
[78] Andy Yee, "China: Qian Yunhui's Death and the Role of Citizen Investigation," Global Voices, January 5, 2011, http://globalvoicesonline.org/2011/01/05/china-qian-yunhui%E2%80%99s-death-and-the-role-of-citizen-investigation/.
[79] Jason Ng, "Zhong Wen Twitter Yong Hu Qun Chou Yang Diao Cha" [Investigation of Random Sampling in Chinese Twitter Users], [*Kenengba*, January 27, 2010, http://www.kenengba.com/post/2540.html (in Chinese).

against the "evil river crab" in an allegory and play on words aimed at voicing discontent with the effects of the government's antipornography campaign.[80]

Overtly political organizations, ethnic minorities, and persecuted religious groups like Falun Gong remain underrepresented among websites that are freely accessible within China, though they have been able to use some ICTs to advance their causes. Charter 08, a prodemocracy manifesto published in December 2008 that calls for multiparty democracy, a free press, and an independent judiciary, garnered 7,000 signatures despite being targeted by censors. Police intimidation and repeated blog shutdowns have not prevented Woeser, a Beijing-based Tibetan blogger, from emerging as an important voice for Tibetan rights, and a source of information on events in the tightly controlled Tibetan region since 2008. After being driven underground by a violent persecutory campaign, adherents of the Falun Gong spiritual practice have used the internet and mobile phones to maintain contact with one another, communicate with overseas practitioners, and download censored information for inclusion in offline leaflets and video discs that expose rights violations and cast doubt on party propaganda. Meanwhile, overseas groups such as Radio Free Asia, Human Rights in China, and the *Epoch Times* have reportedly sent millions of e-mails into the country, supplying users with news summaries on Chinese and international events, instructions on anticensorship technology, and copies of banned publications like former CCP leader Zhao Ziyang's memoir, the *Nine Commentaries*, or the prodemocracy *Beijing Spring* magazine.

VIOLATIONS OF USER RIGHTS

Article 35 of the Chinese constitution guarantees freedoms of speech, assembly, association, and publication, but such rights are subordinated to the national interest and the CCP's status as the ruling power. In addition, the constitution cannot, in most cases, be invoked in courts as a legal basis for asserting rights. The judiciary is not independent and closely follows party directives, particularly in politically sensitive freedom of expression cases. A wide variety of regulations have been issued by different government agencies to establish censorship guidelines. In one recent change, the National People's Congress in April 2010 adopted an amendment to the State Secrets Law[81] that requires telecom operators and ISPs to cooperate with authorities on investigations involving the leaking of state secrets.[82] The law took effect on October 1 and has been generally met with compliance from companies, mostly because the economic stakes of disobedience and loss of business license are so high.

[80] Michael Wines, "A Dirty Pun Tweaks China's Online Censors," *New York Times*, March 11, 2009, http://www.nytimes.com/2009/03/12/world/asia/12beast.html.

[81] "Zhong Hua Ren Min Gong He Guo Zhu Xi Ling, Di Er Shi Ba Hao" [The President Order of The People's Republic of China, No.28], http://www.gov.cn/flfg/2010-04/30/content_1596420.htm (in Chinese).

[82] Reporters Without Borders, "Amendment Enlists ICT Companies in Protectino of State Secrets," news release, April 29, 2010, http://en.rsf.org/china-amendment-enlists-ict-companies-in-29-04-2010,37238.html; Jonathan Ansfield, "China Passes Tighter Information Law," *New York Times*, April 29, 2010, http://www.nytimes.com/2010/04/30/world/asia/30leaks.html.

Although most of these entities already work closely with security services, the move was widely seen as an attempt to reinforce companies' legal liability should they refuse to comply with official requests.

Vague provisions in the criminal code and state-secrets legislation have been used to imprison citizens for their online activities, including publication of articles criticizing the government or exposing human rights abuses, transmission of objectionable e-mail messages, and downloading of censored material from overseas websites. Trials and hearings lack due process, often amounting to little more than sentencing announcements.

In one of the most high-profile free expression cases in recent years, democracy advocate and Nobel Peace Prize laureate Liu Xiaobo was sentenced in December 2009 to 11 years in prison on charges of "inciting subversion of state power" after drafting and circulating the prodemocracy manifesto Charter 08. Six of his online prodemocracy writings, in addition to the manifesto itself, were cited as part of the verdict.[83] Activist Huang Qi was sentenced in November 2009 to three years in prison for "possessing state secrets," having published online criticism of the authorities' response to the 2008 Sichuan earthquake.[84] Tan Zuoren, who had coordinated citizen efforts to document the death toll from school collapses during the quake, was sentenced in February 2010 to five years in prison on charges of "inciting subversion." Rather than basing the charges on his earthquake-related work, however, judges cited a series of e-mail messages sent in 2007 about the 1989 Tiananmen crackdown, an indication of the extent of electronic surveillance even grassroots activists may face.[85] In December 2009, Zhao Lianhai, whose child had fallen sick from melamine-contaminated milk powder, was arrested and charged with "inciting social disorder" after he set up a website called "Home of the Kidney Stone Baby" (http://www.jieshibaobao.com) that advocated for the rights of victimized families.[86] Zhao's trial was held in March 2010 and lasted over five hours, but no verdict was announced.[87] On November 10, 2010, Zhao was sentenced to 30 months in prison,[88] but was subsequently released on medical parole the following month.[89]

---

[83] Sharon Hom, "Google and Internet Control in China: A Nexus Between Human Rights and Trade?" (testimony, U.S. Congressional-Executive Commission on China, Washington, DC, March 24, 2010), http://www.cecc.gov/pages/hearings/2010/20100324/homTestimony.pdf?PHPSESSID=0e7517d795355cc4cd7132dcb51f2004.

[84] Jane Macartney, "Chinese Quake Activist Huang Qi Jailed on 'Secrets' Charges," *Times* (London), November 24, 2009, http://www.timesonline.co.uk/tol/news/world/asia/article6928412.ece.

[85] Reuters, "Chinese Advocate of Quake Victims Sentenced Over E-Mails," *New York Times*, February 8, 2010, http://www.nytimes.com/2010/02/09/world/asia/09china.html.

[86] Tania Branigan, "Chinese Tainted Milk Campaigner Accused of Provoking Social Disorder," *Guardian*, February 3, 2010, http://www.guardian.co.uk/world/2010/feb/03/china-contaminated-milk-campaign-social-disorder; " Zhao Lianhai: Bei Pan You Zui de Jie Shi Ba Ba" [Zhao Lianhai: The Guilty Dad of the Kidney Stone Baby], *Tennis BBS,* March 30, 2010, http://bbs.tennis.com.cn/NewsDetail.asp?GroupName=%B9%E0%CB%AE&dp=60&lp=2&id=11023294 (in Chinese).

[87] "Jie Shi Bao Bao Zhi Fu Zhao Lianhai Shou Kao Jiao Liao Shang Fa Ting" [Kidney Stone Baby Zhao Lianhai Handcuffed at Trial], *Radio France Internationale – Chinese*, March 30, 2010, http://www.chinese.rfi.fr/node/17712 (in Chinese); http://yp.com.hk/iypbusiness_e09/ch/html/news_search/news_ch.aspx?video_id=30499.

Members of religious and ethnic minorities are also targeted for their online activities. In the aftermath of ethnic violence in Xinjiang in July 2009, the authorities arrested the managers of websites reporting on Uighur issues or serving as forums for discussion between Han and Uighurs, including Ilham Tohti, Hailaite Niyazi (a.k.a. Gheyret Niyaz), and Dilixiati Paerhati. Tohti was released after six weeks, but[90] Niyazi was sentenced to 15 years of imprisonment in July on charges of "endangering state security" and the whereabouts of Paerhati remained unclear as of the end of 2010.[91] In December 2010, news emerged that eight months earlier, two individuals working for the Uighur-language website Salkin were sentenced to life imprisonment for translating and reposting an online appeal to protest Han-Uighur clashes at a factory in Guangdong province in July 2009.[92] Tibetans and Falun Gong practitioners who transmit information abroad often suffer repercussions, while some have been arrested solely for accessing or quietly disseminating banned information. In August 2009, 19-year-old Pasang Norbu was reportedly detained at a Lhasa cybercafe after looking at online photos of the Dalai Lama and the Tibetan flag.[93]

In recent years, local officials have increasingly resorted to criminal defamation charges to detain, and in some cases imprison, whistleblowers who post corruption allegations online. In one high-profile case, online activist Wu Baoquan was sentenced in September 2009 to 18 months in prison for defamation after he posted allegations that local officials in Inner Mongolia had forced people off their land and then reaped the profits from its sale to developers. In another case, authorities detained six bloggers in Fujian province in July 2009 after they reported that a young woman had died after being gang-raped by individuals with ties to local officials and criminal groups. While some of the bloggers were released, three—Fan Yanqiong, Wu Huaying, and You Jingyou—were sentenced in April 2010 to between one and two years in prison on charges of posting "false allegations with

[88] Christopher Bodeen, "China food safety activist given 2 1/2 years," Yahoo News, November 10, 2010, http://news.yahoo.com/s/ap/20101110/ap_on_re_as/as_china_tainted_milk_trial.
[89] "Jailed China Milk Activist Free on Parole, Supporters Worry," Sino Daily, December 29, 2010, http://www.sinodaily.com/reports/Jailed_China_milk_activist_free_on_parole_supporters_worry_999.html.
[90] Michael Wines, "Without Explanation, China Releases 3 Activists," *New York Times*, August 23, 2009, http://www.nytimes.com/2009/08/24/world/asia/24china.html.
[91] "China Sentences Uighur Journalist to 15 years," Committee to Protect Journalists, July 26, 2010, http://cpj.org/2010/07/china-sentences-uighur-journalist-to-15-years.php; "A Public Letter by Chinese Citizens Urging the Release of Uyghur Journalist Hailaite Niyazi," Chinese Human Rights Defenders (CHRD), http://chrdnet.org/2010/07/30/a-public-letter-by-chinese-citizens-urging-the-release-of-uyghur-journalist-hailaite-niyazi/; "Scholars Call for Release of Reporter to Respect Freedom of Expression," CVN Beijing, July 30, 2010, http://news.boxun.com/news/gb/china/2010/07/201007302150.shtml.
[92] Edward Wong, "Editor Said to Get Life Sentence for Uighur Reports," *New York Times,* December 24, 2010, http://www.nytimes.com/2010/12/25/world/asia/25uighur.html?_r=1&scp=11&sq=china&st=nyt.
[93] Reporters Without Borders, "Authorities Tighten Grip on Tibetan Websites and Readers," news release, September 9, 2009, http://en.rsf.org/china-authorities-tighten-grip-on-09-09-2009,34434.html; Reporters Without Borders, "Three Years in Jail for Posting Dalai Lama Photos Online," news release, December 4, 2009, http://en.rsf.org/china-three-years-in-jail-for-posting-04-12-2009,34808.

intent to harm."[94] In late 2010, several cases also emerged of individuals facing prosecution and imprisonment for posting to social-networking platforms. Most notably, in November, Cheng Jianping was sentenced without trial to one year in a "re-education through labor" camp in Henan province for sending a Twitter message that mocked anti-Japanese nationalists by jokingly suggesting they attack the Japanese Pavilion at the Shanghai World Expo.[95] Later that month, Beijing activist Bai Dongping was detained on charges of "inciting subversion" for posting a photo of the 1989 Tiananmen Square crackdown on the popular online forum and chat service QQ; the results of his case were pending at year's end.[96]

According to Reporters Without Borders, at least 70 people were in jail for internet-related reasons as of February 2010, compared with 49 known cases in 2008, though the actual number of detainees is likely much higher.[97] Moreover, prison sentences for online violations tend to be longer in China than in many other countries, often a minimum of three years and sometimes as long as life imprisonment, while punishments elsewhere typically range from six months to four years. Once in custody, detainees frequently suffer abuse, including torture and denial of medical attention. Though the targeted individuals represent a tiny percentage of the overall user population, the harsh sentencing of prominent figures has a chilling effect on the fairly close-knit activist and blogging community, and encourages self-censorship among the broader public.

More common than long-term imprisonment are various forms of extralegal harassment. According to some estimates, thousands of individuals have been summoned for questioning and warned in recent years by security officials, employers, or university representatives.[98] For instance, Beijing-based blogger and lawyer Liu Xiaoyuan was contacted by the Justice Bureau in February 2009 because of his online writings in favor of direct elections in the Beijing Lawyer Association.[99] Individuals are also regularly taken into detention and held for several days before being released. Such incidents periodically spark a public outcry online, leading to official compensation for the detainee. In March 2009, for example, 24-year-old Wang Shuai Di was detained for eight days for posting satirical articles with photographs criticizing illegal land requisition in Henan Lingbao County.[100] His case

[94] Reporters Without Borders, "Prison Sentences for Three Bloggers Who Exposed Gang-Rape," news release, April 16, 2010, http://en.rsf.org/china-prison-sentences-for-three-16-04-2010,37058.html.
[95] Andrew Jacobs, "Chinese Woman Imprisoned for Twitter Message," *New York Times,* November 18, 2010, http://www.nytimes.com/2010/11/19/world/asia/19beijing.html?ref=world.
[96] Amnesty International, "China Urged to Release Activist Detained Over Tiananmen Photograph," news release, December 1, 2010, http://www.amnesty.org/en/news-and-updates/china-urged-release-activist-detained-over-tiananmen-photograph-2010-12-01.
[97] Reporters Without Borders, "Internet Censorship Reaches Unprecedented Level," news release, February 23, 2010, http://en.rsf.org/china-internet-censorship-reaches-23-02-2010,36520.html.
[98] Cara Anna, "China's Troublemakers Bond Over 'Drinking Tea,'" Associated Press, March 10, 2010, http://abcnews.go.com/Technology/wirestory?id=10062829&page=1.
[99] Oiwan Lam, "China: Beijing Blogger-Lawyer Liu Xiaoyuan Harassed by Authority," Global Voices Advocacy, February 18, 2009, http://advocacy.globalvoicesonline.org/2009/02/18/china-beijing-blogger-lawyer-liu-xiaoyuan-harassed-by-authority/.
[100] Oiwan Lam, "China: Netizen Jailed for 8 Days for Mocking Local Government," Global Voices Advocacy, April 16, 2009, http://advocacy.globalvoicesonline.org/2009/04/16/china-netizen-jailed-for-8-days-for-mocking-local-government/.

soon attracted attention from both the online community and traditional media, and he eventually won an apology from the police and 783.93 yuan (US$115) in compensation.[101] In August 2009, blogger Guo Baofeng, one of those detained in connection with the Fujian rape case, was released following a postcard-writing campaign initiated by fellow online activists.[102] Other forms of harassment include restrictions on travel, particularly travel abroad, a measure employed with greater frequency in the run-up to the Nobel Peace Prize ceremony in Oslo, as authorities feared Liu's acquaintances would seek to attend on his behalf. Though physical violence against bloggers is unusual, one such incident drew widespread attention in February 2009. Blogger Xu Lai was stabbed in the stomach by unknown assailants after giving a talk at a Beijing bookshop, and comments made by the attackers indicated that the assault was in response to Xu's satirical comments online.[103] In another episode, prominent blogger and artist Ai Weiwei was beaten in the head in August 2009 by police when visiting Chengdu to testify at the trial of fellow online activist Tan Zuoren; the following month, while visiting Germany, Ai required surgery to address a brain hemorrhage that emerged due to the beating.[104]

The space for anonymous online communication in China is steadily shrinking. Despite surveys showing that some 78 percent of users are opposed to real-name registration, the practice has gained ground in recent years.[105] Most major news portals such as Sina, Netease, and Sohu implemented real-name registration for their comment sections during 2009.[106] It had already been required in cybercafes, university BBS, and major blog-hosting sites.[107] An internet content provider (ICP) license from the MIIT is required to establish a personal or corporate website within China, and the process requires applicants

[101] Oiwan Lam, "China: Free Wu Baoquan," Global Voices Advocacy, April 21, 2009, http://advocacy.globalvoicesonline.org/2009/04/21/china-free-wu-baoquan/; Wang Jun Xiu, " Lingbao Shi Gong An Ju Xiang Guan Fu Ze Ren Bei Chu Li, Wang Shuai Huo Pei 783.93 Yuan" [Lingbao County Police Officer Dismissed; Wang Shuai Compensated 783.93 Yuan], April 18, 2009, http://china.rednet.cn/c/2009/04/18/1746296.htm (in Chinese).

[102] Guobin Yang, "The Curious Case of Jia Junpeng, or The Power of Symbolic Appropriation in Chinese Cyberspace," *The China Beat*, October 20, 2009, http://www.thechinabeat.org/?cat=144; "Postcard Campaign for Detainees," Radio Free Asia, August 5, 2009, http://www.rfa.org/english/news/china/postcardcampaign-08052009094856.html.

[103] Tania Branigan, "Chinese Blogger Xu Lai Stabbed in Beijing Bookshop," *Guardian*, February 15, 2009, http://www.guardian.co.uk/world/2009/feb/15/china-blogger-xu-lai-stabbed.

[104] Ed Vulliamy, "Ai Weiwei: The rebel who has suffered for his art," *Guardian*, October 10, 2010, http://www.guardian.co.uk/theobserver/2010/oct/10/ai-weiwei-artist-ed-vulliamy

[105] "Hu Lian Wang Shi Min Zhi Ying Fa Zhuan Jia Ji Bian" [Internet Real Name System Causes Debate Among Experts], *Sina News Survey*, July 24, 2010, http://news.survey.sina.com.cn/voteresult.php?pid=3101 (in Chinese).

[106] Jonathan Ansfield, "China Web Sites Seeking Users' Names," *New York Times*, September 5, 2009, http://www.nytimes.com/2009/09/06/world/asia/06chinanet.html; Reporters Without Borders, "Government Crusade Against Online Anonymity," news release, May 7, 2010, http://en.rsf.org/china-government-crusade-against-online-07-05-2010,37412.html.

[107] "Wen Hua Bu 2009 Jiang Da Li Zhen Zhi Hu Lian Wang Di Su Zhi Feng" [Ministry of Culture Will Curb Trend of Internet Indecency in 2009], *Net Bar China*, January 6, 2009, http://www.netbarcn.net/Html/PolicyDynamic/01061954388252.html (in Chinese); Chen Jung Wang, "Shi Min Zhi Rang Gao Xiao BBS Bian Lian" [Real Name System Intimidates High School BBS], *CNHubei*, November 29, 2009, http://www.cnhubei.com/200511/ca936578.htm (in Chinese); "Zhong Guo Hu Lian Xie Hui: Bo Ke Tui Xing Shi Min Zhi Yi Chen Ding Ju" [Internet Society of China: Real Name System for Bloggers is Set], *Xinhua News,* October 22, 2006, http://www.itlearner.com/article/3522 (in Chinese).

to submit personal identification information. Throughout 2009, the ministry tightened enforcement of this requirement,[108] reportedly leading to the shutdown of 130,000 websites and especially affecting self-employed workers or freelancers.[109] In February 2010, the authorities added a requirement that individuals registering a website have their photograph taken and placed on file.[110]

Prior to September 2010, SIM cards for mobile phones could be purchased anonymously, though the transmission of text messages could still be monitored. In late August 2010, MIIT confirmed that beginning September 1, all SIM card purchasers would be required to register with valid ID documents. For users possessing anonymous SIM cards (around 320 million), telecom operators are obliged to help them register within three years.[111] The purported reasons for the MIIT to take such measures are the prevalent transmission of fraudulent, pornographic, or spamming messages over mobile phones, but the steps also raised fears of a potential crackdown on those transmitting politically sensitive content. Separately, in January 2010, China Mobile's Shanghai branch announced that it would begin suspending a mobile phone's text-messaging function if the user was found to be distributing "vulgar," "pornographic," or "other illegal content."[112]

Surveillance of internet communication by security forces is pervasive,[113] and in recent years they have focused additional resources on advanced web applications. During the 2009 National Conference for Politics and Legislative Affairs, the Ministry of Public Security proposed strengthening surveillance and control of microblogging and QQ instant-messaging groups, which it considered a seedbed for social unrest.[114] In some free expression cases—such as that of democracy activist Guo Quan, sentenced in October 2009

[108] Oiwan Lam, "China: Unlicensed Websites Expelled and Blocked," Global Voices Advocacy, March 4, 2009, http://advocacy.globalvoicesonline.org/2009/03/04/china-unlicensed-websites-expelled-and-blocked/; "ICP License Crackdown," *China Hosting Blog*, December 6, 2009, http://blog.sinohosting.net/icp-license-crackdown/.

[109] Rebecca MacKinnon, "Google and Internet Control in China."

[110] Donnie Hao Dong, "Wanna Setup a Personal Website in China? BEING TAKEN a Portrait Please," *Blawgdog*, February 23, 2010, http://english.blawgdog.com/2010/02/wanna-setup-personal-website-in-china.html; Elinor Mills, "China Seeks Identity of Web Site Operators," CNET News, February 23, 2010, http://news.cnet.com/8301-27080_3-10458420-245.html.

[111] " Shou Ji Shi Ming Zhi Jin Qi Shi Shi, Gou Ka Xu Chi Shen Fen Zheng" [Mobile phone real name system implemented today, SIM card purchasers have to present their ID documents], News 163, October 1, 2010, http://news.163.com/10/0901/00/6FF3HKF8000146BD.html (in Chinese).

[112] Yeh Feng and Ji Ming, "Shanghai Yi Dong: Shou Ji Fa Song Huang Se Duan Xin Yi Jing Fa Xian Jiang Ting Zhi Duan Xin Gong Neng" [China Mobile Shanghai Branch: Mobile Phone's Text Messaging Function Will be Suspended If Users Found Sending Vulgar Messages], *Xinhua News,* January 18, 2010, http://news.xinhuanet.com/politics/2010-01/18/content_12833023.htm (in Chinese); Sharon Lafraniere, "Text Messages in China to Be Scanned for 'Illegal Content,'" *New York Times*, January 19, 2010, http://www.nytimes.com/2010/01/19/technology/20text.html; People.Com http://ccnews.people.com.cn/GB/10793560.html ; Sina debate on real name registration, http://tech.sina.com.cn/focus/NetID_2005/index.shtml; http://www.dw-world.de/dw/article/0,,5150374,00.html; http://0763f.com/weekly/dubao/2010/0122/11308.html.

[113] Ethan Gutmann, "Hacker Nation: China's Cyber Assault," *World Affairs* (May/June 2010), http://www.worldaffairsjournal.org/articles/2010-MayJune/full-Gutmann-MJ-2010.html.

[114] "Gong An Bu Jiang Jia Qiang Wei Bo QQ Qun Jian Kong Ying Dui Xing Mei Ti Ying Xiang" [New Media Faces Consequences of Increasing Control of Microblogging and QQ by the Ministry of Public Security], *Wu Han Evening News*, January 6, 2010, http://china.huanqiu.com/roll/2010-01/680180.html (in Chinese).

to 10 years in prison for attempting to organize a political party—private instant-messaging conversations or text messages have been directly cited in court documents.[115]

China has emerged as a key global source of cyberattacks. Although not all attacks originating in the country have been explicitly traced back to the government, their scale, organization, and targets have led many experts to believe that they are either sponsored or condoned by Chinese military and intelligence agencies. The assaults have included denial-of-service attacks on domestic and overseas groups that report on human rights abuses, such as Human Rights in China, Aizhixing, Boxun, Falun Gong websites, ChinaAid, and Chinese Human Rights Defenders.[116] Another notable target was the July 2009 Melbourne Film Festival, which showed a film about Uighur activist Rebiya Kadeer. Some attacks have taken the form of e-mail messages to foreign correspondents and activists that carry malicious software capable of spying on the recipient's computer.[117] There have also been large-scale hacking attacks designed to access the Gmail accounts of Chinese human rights activists and other information hosted by over 30 financial, defense, and technology companies, mostly based in the United States.[118] Extensive cyberespionage networks have been detected extending to 103 countries in an effort to spy on the Tibetan government-in-exile and its contacts, including Indian government facilities and foreign embassies.[119]

[115] The verdict against Guo Quan is available in English on the Dui Hua Foundation website at http://www.duihua.org/work/verdicts/verdict_Guo%20Quan_en.htm.

[116] Maggie Shiels, "Security Experts Say Google Cyber-Attack Was Routine," BBC, January 14, 2010, http://news.bbc.co.uk/2/hi/technology/8458150.stm; Gutmann, "Hacker Nation;" Persecution.org, "ChinaAid Websites Collapse Under Repeated Malicious Cyber Attacks," December 2, 2010, http://www.persecution.org/2010/12/02/chinaaid-websites-collapse-under-repeated-malicious-cyber-attacks/.

[117] Andrew Jacobs, "Journalists' E-Mails Hacked in China," *New York Times*, March 30, 2010, http://www.nytimes.com/2010/03/31/world/asia/31china.html; Andrew Jacobs, "I Was Hacked in Beijing," *New York Times*, April 9, 2010, http://www.nytimes.com/2010/04/11/weekinreview/11jacobs.html.

[118] Andrew Jacobs and Miguel Helft, "Google, Citing Attack, Threatens to Exit China," *New York Times*, January 12, 2010, http://www.nytimes.com/2010/01/13/world/asia/13beijing.html; Ariana Eunjung Cha and Ellen Nakashima, "Google China Cyberattack Part of Vast Espionage Campaign, Experts Say," *Washington Post*, January 14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.

[119] Information Warfare Monitor and Shadowserver Foundation, "Shadows in the Cloud: Investigating Cyber Espionage 2.0," April 6, 2010, http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0; Information Warfare Monitor, "Tracking Ghostnet: Investigating a Cyber Espionage Network," March 29, 2009, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

CUBA

	2009	2011
INTERNET FREEDOM STATUS	Not Free	Not Free
Obstacles to Access	25	24
Limits on Content	30	30
Violations of User Rights	33	33
Total	88	87

POPULATION: 11.3 million
INTERNET PENETRATION: 1 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Despite a slight loosening of restrictions on the sale of computers in 2008 and the important growth of mobile-phone infrastructure in 2009 and 2010, Cuba remains one of the world's most repressive environments for the internet and other information and communication technologies (ICTs). There is almost no access to internet applications other than e-mail, and surveillance is extensive, including special software designed to monitor and control many of the island's public internet-access points.[1] Nevertheless, a growing community of bloggers has consolidated their work, creatively using online and offline means to express opinions and spread information about conditions in the country.

Cuba was connected to the internet for the first time in 1996, and the National Center for Automated Interchange of Information (CENIAI), the country's first internet-service provider (ISP), was established that year. However, the executive authorities continue to control the legal and institutional structures that decide who has access to the internet and how much access will be permitted.[2]

OBSTACLES TO ACCESS

According to the last official report on the website of the National Statistics Office, there

[1] "Prestaciones efectivas para redes informáticas" [Effective Features for Computer Networks], Radio Surco, April 11, 2009, http://www.radiosurco.icrt.cu/Ciencia.php?id=415; Danny O'Brien, "The Malware Lockdown in Havana and Hanoi,"*CPJ Blog*, June 8, 2010, http://cpj.org/blog/2010/06/the-malware-lockdown-in-havana-and-hanoi.php.
[2] Ben Corbett, *This Is Cuba: An Outlaw Culture Survives* (Cambridge, MA: Westview Press, 2002), 145.

were 1.6 million internet users in Cuba in 2009, representing 14.2 percent of the population.[3] However, only 2.9 percent of Cubans access the internet regularly and 5.8 percent routinely use email. Most internet users are only able to connect to a government intranet rather than the internet proper. Some sources estimate that only 200,000 residents have access to the world wide web.[4]

Most individuals who are able to access internet face extremely slow connections, making the use of multimedia applications nearly impossible. In January 2010, the government announced that it had expanded the national bandwidth and achieved a 10 percent increase in international connectivity. According to official data, Cuba now has speeds of 209 megabits per second (Mbps) for downloading and 379 Mbps for uploading. [5] However, these high-speed connections are not available to regular users and officials also noted that the government's plans did not include fostering private use of the internet.

Cuba continues to blame the U.S. embargo for its connectivity problems, saying it must use a slow, costly satellite connection system and is limited in the space it can buy. But in 2009, in a move that eased some aspects of Washington's prolonged sanctions on trade with Cuba, President Barack Obama allowed U.S. telecommunications firms to enter into agreements to establish fiber-optic cable and satellite telecommunication facilities linking the United States and Cuba and to enter into roaming agreements with Cuban providers.[6] Cuba's leaders reiterated their demand for a complete end to the embargo, and official media ignored this important change in the U.S. legal framework. The bilateral relationship was affected by another incident in 2009 that touched directly on the lack of open internet access in Cuba. On December 4, the Cuban authorities arrested an American independent contractor, Alan Gross, who was in the country to set up individual satellite-based internet connections as part of a U.S. government–funded project.

The Cuban government maintains tight control over the sale and distribution of internet-related equipment. The sale of modems was banned in 2001, and the sale of computers and computer accessories to the public was banned in 2002. This policy changed in early 2008, when the government began allowing Cubans to buy personal computers, and individuals can now legally connect to an ISP with a government permit. However, this permit is granted only to certain people, mostly Cuban officials or "trusted journalists." High costs also put internet access beyond the reach of most of the population. A simple

[3] National Statistics Office, Republic of Cuba, *Tecnologías de la Información y las Comunicaciones en Cifras: Cuba 2009* [Information and Communication Technologies in Figures: Cuba 2009] (Havana: National Statistics Office, May 2010), http://www.one.cu/ticencifras2009.htm.

[4] Ray Sanchez, "Cuba Cutting Internet Access," *Sun Sentinel*, May 7, 2009, http://www.sun-sentinel.com/news/nationworld/sfl-cuba-internet-cutoff-050709,0,4376220.story; Reporters Without Borders, http://www,rsf.irg/article.php3?!id_article26096.

[5] Amaury E. del Valle, "Cuba, la red sigue creciendo" [Cuba, the Network Continues to Grow], *Juventud Rebelde*, January 6, 2010, http://www.juventudrebelde.cu/suplementos/informatica/2010-01-06/cuba-la-red-sigue-creciendo/.

[6] "Fact Sheet: Reaching Out to the Cuban People," The White House: Office of the Press Secretary, April 13, 2009, http://www.whitehouse.gov/the_press_office/Fact-Sheet-Reaching-out-to-the-Cuban-people.

computer with a monitor averages around 722 convertible pesos (US$780) in retail outlets, or at least 550 convertible pesos (US$594) on the black market.[7] By comparison, the average monthly Cuban salary is approximately 16 convertible pesos (US$17).[8] Computers are generally distributed by the state-run Copextel Corporation, which imports ICT equipment. Approximately 31 percent of Cubans report having access to a computer, but 85 percent of those said that the computers were located at work or school.[9] An internet connection in a hotel costs between 6 and 12 convertible pesos per hour.

Cuba still has the lowest mobile-phone penetration rate in Latin America, but the number is rising fast. There were 443,000 active mobile-phone subscriptions in 2009, a huge increase since 2004 when that figure was approximately 75,400.[10] In part because family members frequently share a mobile phone, it is estimated that the total number of users currently exceeds one million.[11] The government eased restrictions on mobile-phone purchases in March 2008, and reduced the sign-up fee by more than half, though it still represents three months' wages for the average worker.

In another step to increase affordability, the state-owned telecommunications firm ETECSA announced a series of rate modifications in April 2010.[12] Per-minute rates for calls on prepaid accounts will be reduced from 0.65 convertible pesos to 0.45 convertible pesos, except for 11:00 p.m. to 7:00 a.m., when a 0.10 convertible peso rate will apply. Also, international long-distance rates will fall, for both mobile and fixed-line accounts, by between 42 and 75 percent. Calls to the Western Hemisphere will now cost 1.60 convertible pesos per minute, except for the United States (1.85) and Venezuela (1.40), and calls to the rest of the world will be 1.80 per minute.[13] In addition, a scheme will be introduced whereby either the caller or the call recipient will be able to indicate that they will pay the entire charge for a call. Ordinarily, both parties to a call pay 0.45 convertible pesos per minute, but under the new scheme, the party taking on the whole charge will pay 0.60 convertible pesos per minute.

Activation fees for new accounts have fallen from 120 to 60 to 40 convertible pesos. Cuba has roaming agreements with 306 carriers in 128 countries, and 2.2 million people

[7] "Cubans Queue for Computers as PC Ban Lifted, But Web Still Outlawed," *Irish Examiner*, May 5, 2008.
[8] "Mobile Phone Use Booms in Cuba Following Easing of Restrictions," Agence France-Presse, April 24, 2008.
[9] [9] National Statistics Office, Republic of Cuba, *Tecnologías de la Información y las Comunicaciones en Cifras: Cuba 2009* [Information and Communication Technologies in Figures: Cuba 2009]
[10] There were 327,000 subscriptions in 2007. International Telecommunications Union (ITU), "ICT Statistics 2009—Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/CellularSubscribersPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.
[11] "ETESCA mobile phone users cross million mark," cubastandard.com, July 14, 2010 http://www.cubastandard.com/2010/07/14/etecsa-mobile-phone-users-cross-million-mark.
[12] The website of ETECSA, or Empresa de Telecomunicaciones de Cuba SA, can be found at http://www.enet.cu .
[13] Amaury E. del Valle, "Rebajarán tarifas para llamadas de telefonía móvil en Cuba" [Prices for Mobile Telephone Calls Will Fall in Cuba], *Juventud Rebelde*, April 21, 2010, http://www.juventudrebelde.cu/suplementos/informatica/2010-04-21/rebajaran-tarifas-para-llamadas-de-telefonia-movil-en-cuba/.

used those services in Cuba in 2010.[14] The island's mobile network already covers 70 percent of Cuban territory, and further expansions are planned.[15] Most mobile phones do not include internet connections, but it is possible to send and receive international text messages and photographs with certain phones.

In November 2010, after a series of delays, the government announced that the fiber-optic cable being installed between Cuba, Venezuela, and Jamaica to improve the island's internet connection would become available in January 2011. When the cable becomes fully functional, it is expected to dramatically improve the internet speed on the island and make it easier to access multimedia content. However, it is unlikely that the cable will enable significant network expansion and bring the internet to a greater number of Cubans.[16]

The government divides access to web technology between the national intranet and the global internet. Most Cubans only have access to the former, which consists of a national e-mail system, a Cuban encyclopedia, a pool of educational materials and open-access journals, Cuban websites, and foreign websites that are supportive of the Cuban government.[17] Cubans can legally access the internet only through government-approved institutions, such as the approximately 600 Joven Clubs de Computación (Youth Computer Clubs) and points of access run by ETECSA.[18] Users are generally required to present identification to use computers at these sites. Many neighborhoods in the main cities of Havana and Santiago advertise "internet" access in ETECSA kiosks, but field research has found that the kiosks often lack computers, instead offering public phones for local and international calls with prepaid phone cards. The government also claims that all schools have computer laboratories, while in practice internet access is usually prohibited for students or limited to e-mail and supervised activities on the national intranet.

In June 2009, the government adopted a new law (Resolution No. 99/2009) allowing the Cuban Postal Service, which is controlled under the domain of the Ministry of Computers and Communications, to establish cybercafes at its premises and offer internet access to the public.[19] However, home connections are not yet allowed for the vast majority of Cubans and only those favored by the government are able to access the internet from their own homes.

One segment of the population that enjoys approved access to the internet is the professional class of doctors, professors, and government officials. Facilities like hospitals, polyclinics, research institutions, and local doctors' offices are linked by an online network called Infomed. However, even these users are typically restricted to e-mail and sites related

[14] Ibid.
[15] Nick Miroff, "Getting Cell Phones Into Cuban Hands," Global Post, May 17, 2010, http://www.globalpost.com/dispatch/cuba/100514/cell-phone.
[16] Ellery Biddle, "Cuba: Fiber Optic Cable May Not Bring Greater Internet Access," Global Voices, November 19, 2010, http://globalvoicesonline.org/2010/11/19/cuba-fiber-optic-cable-may-not-bring-greater-internet-access/.
[17] ETECSA: Empressa de Telecomunicaciones de Cuba S.A., www.enet.cu, Accessed August 28, 2010.
[18] See the club system's website at http://www.cfg.jovenclub.cu/.
[19] Resolution No. 99/2009 was published in the Official Gazette on June 29, 2009)

to their occupations. Beginning in 2007, the government systematically blocked core internet portal sites such as Yahoo!, MSN, and Hotmail. This ban was extended to blog platforms and blog commentary technology during certain periods in 2008. As a result, Cubans cannot access blogs written by their fellow citizens. Moreover, Voice over Internet Protocol (VoIP) remains blocked in Cuba, with the exception of unauthorized points of connection in old Havana. Some social-networking platforms such as Facebook and Twitter are accessible in university cybercafes and other location, although with varying consistency.

There are only two ISPs, CENIAI Internet and ETECSA, and both are owned by the state. Cubacel, a subsidiary of ETECSA, is the only mobile-phone carrier. In 2000, the Ministry of Information Science and Communication was created to serve as the regulatory authority for the internet, and its Cuban Supervision and Control Agency oversees the development of internet-related technologies.[20]

LIMITS ON CONTENT

Rather than engaging in the technically sophisticated blocking and filtering used by other repressive regimes in countries like China and Tunisia, Cuban authorities rely heavily on lack of technology and prohibitive costs to limit users' access to information. The websites of foreign news outlets—including the British Broadcasting Corporation (BBC), *Le Monde*, and *El Nuevo Herald* (a Miami-based Spanish-language daily)—and human rights groups like Amnesty International, Human Rights Watch, and Freedom House remain largely accessible, though slow connection speeds impede access to the content on these sites.[21] Some sites and writings that are considered anti-Cuban or counterrevolutionary are restricted. These include many of the Cuban dissident sites based in the United States and abroad, and any documents containing criticism of the current system or mentioning dissidents, supply shortages, or other politically sensitive issues.[22] Blogs and other sites with content written by Cubans residing in Cuba—such as the blogging platform Voces Cubanas and the *Bitácora Cubana* blog—are also inaccessible. Sites such as Cubanet.org, Payolibre.com, Cubaencuentro.com, and the Association for Freedom of the Press also cannot be accessed at youth computer centers.[23] Even Revolico.com, a platform for classified advertisements that has no direct association with politics, has been censored.[24]

[20] The ministry's website can be found at http://www.mic.gov.cu/.

[21] Reporters Without Borders, "Free Expression Must Go With Better Communications, Says Reporters Without Borders as Blogs Prove Hard to Access," news release, March 31, 2008, http://en.rsf.org/cuba-free-expression-must-go-with-31-03-2008,26396.html.

[22] OpenNet Initiative, "Country Profiles: Cuba," May 9, 2007, http://opennet.net/research/profiles/cuba.

[23] *Bitácorea Cubana* can be found at http://cubabit.blogspot.com/; the Association for Freedom of the Press (Asociación pro Libertad de Prensa) can be found at http://prolibertadprensa.blogspot.com/.

[24] Marc Lacy, "A Black Market Finds a Home in the Web's Back Alleys," *New York Times*, January 3, 2010, http://www.nytimes.com/2010/01/04/world/americas/04havana.html.

It is a crime to contribute to international media that are not supportive of the government, a fact that has led to widespread self-censorship. Cuban blogs typically feature implicit or explicit elements of self-censorship and anonymity. Many of those working closely with ICTs are journalists who have been barred from official employment, and the prohibitive costs surrounding the technology represent a major obstacle for them. The majority of their work is done offline by hand, typewriter, or computer, then uploaded and published once or twice a week using a paid internet-access card. For those contributing to international outlets, content can be dictated via costly international phone calls.

Despite all of these barriers, Cubans still connect to the internet through both authorized and non-authorized points of access. Some are able to break through the infrastructural blockages by building their own antennas, using illegal dial-up connections, and developing blogs on foreign platforms. The underground economy of internet access also includes account sharing, in which authorized users sell access to those without an official account for one or two convertible pesos per hour. Some foreign embassies allow Cubans to use their facilities, but a number of people who have visited embassies for this purpose have reported police harassment. Some cases of Cuban activists using mobile phones or text messaging to organize events or disseminate political information have been reported. There is a thriving improvisational system of "sneakernets," in which USB keys and data discs are used to distribute material (articles, prohibited photos, satirical cartoons, video clips) that has been downloaded from the internet or stolen from government offices.

There is no exact count of blogs produced in Cuba, but the Cuban Journalists' Union (UPEC) has reported a current total of 174. Examples include Yoani Sánchez's famous blog *Generación Y*, which draws 26 percent of its readers from within Cuba, as well as sites like *Retazos*, Nueva Prensa, and *Convivencia*. Regional radio stations and magazines are also creating online versions, though these are state-run and do not accept contributions from independent journalists. However, in a recent development, some of these sites have installed commentary tools that allow readers to provide feedback and foster discussion, albeit censored.

Yoani Sánchez has become the most visible figure in a blogging movement that uses new media to report on daily life and conditions in Cuba that violate basic freedoms. She and other online writers—including Claudia Cadelo, Miriam Celaya, Orlando Luis Pardo, Reinaldo Escobar, Laritza Diversent, and Luis Felipe Rojas—have come together on the Voces Cubanas blogging platform to portray a reality that the official media ignore, earning broad support throughout society that resulted in the government shutting down the platform. They have even made it "trendy" to exercise the right to free expression. Young people are increasingly using the Twitter microblogging service and mobile phones to document repression, as well as to spread leaks of prohibited information. These have included reports from a closed-door meeting at the Communist Party's Central Committee headquarters, news on freezing and starvation deaths in a psychiatric hospital, and explicit

videos of student protests and police beatings.[25]

Unable to completely suppress dissident activity on the internet through legal and infrastructural constraints, the authorities have taken a number of countermeasures within the medium itself. Government entities maintain a major presence on the social networks, and they have relied on trusted students at the University of Computer Sciences to help fight the "internet campaigns against Cuba." The authorities have also created official blogs designed to slander and criticize the independent bloggers.[26]

VIOLATIONS OF USER RIGHTS

The legal structure in Cuba is not favorable to internet freedom. The constitution explicitly subordinates freedom of speech to the objectives of socialist society,[27] and freedom of cultural expression is guaranteed only if the expression is not contrary to the Revolution.[28] The penal code and Law 88 set penalties ranging from a few months to 20 years in prison for any activities that are considered a "potential risk," "disturbing the peace," a "precriminal danger to society," "counterrevolutionary," or "against the national independence or economy."[29]

In 1996, the government passed Decree-Law 209, which states that the internet cannot be used "in violation of Cuban society's moral principles or the country's laws," and that e-mail messages must not "jeopardize national security."[30] In 2007, Resolution 127 on network security banned the spreading via public data-transmission networks of information that is against the social interest, norms of good behavior, the integrity of people, or national security. The decree requires access providers to install controls that will enable them to detect and prevent the proscribed activities, and to report them to the relevant authorities.

Resolution 56/1999 provides that all materials intended for publication or dissemination on the internet must first be approved by the National Registry of Serial Publications. Moreover, Resolution 92/2003 prohibits e-mail and other ICT service providers from granting access to individuals who are not approved by the government, and requires that they enable only domestic chat services, not international ones. Entities that violate these regulations can have their authorization to provide access suspended or

[25] For example, see the videos of a August 2008 police beating and October 2009 student protest posted on YouTube: http://www.youtube.com/watch?v=L0mztIF8wxE, http://www.youtube.com/watch?v=WLEX6_VAzMo&feature=fvw. Also, pictures of malnutritioned patient bodies from a local hospital on the Penúltimos Días blog http://www.penultimosdias.com/2010/03/02/los-muertos-de-mazorra/.

[26] A few examples include Cambios en Cuba, http://cambiosencuba.blogspot.com/; Yohandry's weblog, http://yohandry.wordpress.com/; and the official bloggers platform CubaSí, http://www.cubasi.cu.

[27] Article 53, available at http://www.cubanet.org/ref/dis/const_92_e.htm, accessed July 23, 2010.

[28] Article 39, d), available at http://www.cubanet.org/ref/dis/const_92_e.htm, accessed July 23, 2010.

[29] Committee to Protect Journalists, "International Guarantees and Cuban Law," special report, March 1, 2008, http://cpj.org/reports/2008/03/laws.php.

[30] Cuba – Telecoms Market Overview & Statistics 2008.

revoked.

Resolution 179/2008 requires all ISPs to censor materials viewed in conflict with state security or contrary to social interests, ethics, and morals. Specifically, it authorizes ETESCA to "take the necessary steps to prevent access to sites whose contents are contrary to social interests, ethics and morals, as well as the use of applications that affect the integrity or security of the State." The resolution, which also spells out the requirements and procedures to become an ISP, requires ISPs to register and retain the addresses of all traffic for at least a year. [31]

Cuban customs regulations specifically prohibit the entry of any phones that use the Global Position System (GPS) or satellite connections.[32] Despite constitutional provisions that protect various forms of communication, and portions of the penal code that set penalties for the violation of the secrecy of communications, the privacy of users is frequently violated in practice. Tools of content surveillance and control are pervasive, from public access points and universities to government offices. The government routes most connections through proxy servers and is able to obtain all user names and passwords through special monitoring software Avila Link, which is installed at most ETECSA and public access points. In addition, delivery of e-mail messages is consistently delayed, and it is not unusual for a message to arrive without its attachments.

The government continues to repress independent journalism and blogging with fines, searches, the confiscation of money and equipment. There have been a few cases in which online journalists were imprisoned for their work, most notably two correspondents for Cubanet.org. One of them was sentenced to four years in prison in April 2007 for "precriminal social danger," and the other was sentenced to seven years in November 2005 for "subversive propaganda." More recent is the case of Dania Virgen Garcia, a blogger and journalist, who was arrested in April 2010 and sentenced to 20 months in prison on arbitrary charges; the authorities released her a few weeks following the arrest.

Prominent bloggers and activists face a variety of other forms of harassment and intimidation. In May 2008, during a public trial of dissident economist Martha Beatriz Roque, state television and *Granma* showed evidence of government hacking of dissidents' Yahoo! accounts.[33] Bloggers have been summoned for questioning, reprimanded, and had their domestic and international travel rights restricted.[34] Luis Felipe Rojas, a blogger who

[31] "Internet En Cuba : Reglamento Para Los Proveedores De Servicos De Acceso A Internet" (Internet in Cuba: Regulations for Internet Service Providers), http://cubanosusa.com/opinion/editorial/42454-internet-en-cuba-reglamento-proveedores-acceso-internet.html, accessed on August 28, 2010.

[32] See the website of Aduana General de la Republica de Cuba (Cuban Customs): http://www.aduana.co.cu/turista.htm.

[33] Deisy Francis Mexidor, "Presentan evidencias irrefutables sobre actividad subversiva de Estados Unidos contra Cuba" [Irrefutable Evidence Is Presented of Subversive Activity Against Cuba], *Granma*, May 19, 2008, http://www.granma.cubaweb.cu/2008/05/19/nacional/artic20.html.

[34] Steven L. Taylor, "Cuba vs. the Bloggers," *PoliBlog*, December 6, 2008, http://www.poliblogger.com/index.php?s=cuba+bloggers; Eduardo Avila, "Cuba: Government Officials Tell Bloggers to Cancel Planned Meeting," Global Voices Advocacy, December 6, 2008, http://advocacy.globalvoicesonline.org/2008/12/06/cuba-government-officials-tell-bloggers-to-cancel-planned-meeting/;

documents human rights abuses, was taken for questioning and detained on numerous occasions, most recently in August 2010.[35] Moreover, in recent years, the Cuban government refused on multiple occasions to issue Yoani Sánchez a travel visa that would have allowed her to receive various prizes or honors overseas.[36] Similarly, in May 2010, the government denied another blogger, Claudia Cadelo, a permission to leave Cuba to attend an international gathering of bloggers in Germany.[37]

Marc Cooper, "Cuba's Blogger Crackdown," *Mother Jones*, December 8, 2008, http://www.motherjones.com/politics/2008/12/cubas-blogger-crackdown.

[35] For more information, see Rojas' blog Crossing the Barbed Wire, http://cruzarlasalambradaseng.wordpress.com/.

[36] "Cuba Refuses to Give Blogger Visa to Collect Prize," Agence France-Presse, May 6, 2008. On Yoani Sanchez being denied visa to Brazil on July 2010 see http://www.google.com/hostednews/epa/article/ALeqM5jSr2TuI94zsTbnak2Il-C-p44gcA.
On Yoani Sánchez denied visa to travel to receive a special recognition from the Maria Moors Cabot Prize committee in New York on October 2009 see, http://www.americasquarterly.org/yoani-sanchez-cabot-award.

[37] Claudia Cadelo, "Confessions Regarding Utopian Journey," translated by Octavo Cerco, May 12, 2010, http://octavocercoen.blogspot.com/2010/05/confessions-regarding-utopian-journey.html

EGYPT

	2009	2011
INTERNET FREEDOM STATUS	Partly Free	Partly Free
Obstacles to Access	13	12
Limits on Content	12	14
Violations of User Rights	26	28
Total	51	54

POPULATION: 80.4 million
INTERNET PENETRATION: 24 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Partly Free

EDITOR'S NOTE:

The following report covers developments in Egypt until December 31, 2010. However, events that have occurred since the end of the coverage period have significantly altered the country's political and internet freedom landscape. On January 25, Egyptians took to the streets as part of widespread protests against President Hosni Mubarak, demanding that he step down.

Social media tools such as Facebook and Twitter played a strategic role in mobilizing citizens and disseminating news. The authorities soon responded with intermittent blocks on access to such tools and to the websites of prominent independent newspapers. Then, in an extreme measure, from January 27 to February 2, the government, cut off all internet access and mobile-phone services in the country. A large number of bloggers and online activists were also detained during the protests, including Google executive Wael Ghonim, who disappeared on January 28, and was released from government detention on February 7.

On February 11, Mubarak stepped down, and the government ceded power to the Egyptian Army, while all detained journalists were freed. However, tensions between citizens and the army have since surfaced. On March 28, military police arrested blogger Maikel Nabil Sanad for criticizing the lack of transparency in the armed forces. On April 11, he was sentenced to three years in prison.

INTRODUCTION

While the Egyptian government has aggressively and successfully sought to expand access to the internet as an engine of economic growth, its security forces have increasingly attempted to curtail the use of new technologies for disseminating and receiving sensitive political information. Rather than relying on technical content filtering or monitoring, they typically employ "low-tech" methods such as intimidation, legal harassment, detentions, and real-world surveillance of online dissidents. The growing crackdown is a response to increased

internet-based activism among Egyptians in the last few years, which has given rise to political opposition movements such as the April 6 Youth Movement and the National Coalition for Change. The authorities' desire to suppress web-based and traditional media became even more evident in advance of the November 2010 parliamentary elections.

The internet was first introduced in Egypt in 1993 through the Egyptian Universities Network and the Egyptian cabinet's Information and Decision Support Center (IDSC). The general public gained access in 1995, but the technology did not really take off until 2002, when the government introduced a "Free Internet" initiative, whereby anyone with a telephone line and a computer could access the internet for the price of a local call (US$0.15 an hour). To date, there are no laws regulating internet use in Egypt, although the government represses internet activism using the Emergency Law, which has been in effect since 1981.

OBSTACLES TO ACCESS

Access to digital communications has grown exponentially since it was first made available to the public in the mid-1990s. According to government statistics, 0.58 percent of the population used the internet regularly in 1999.[1] By the end of 2009, the figure had grown to 24 percent, or 20.1 million users.[2] However, several barriers to access remain, including basic illiteracy, computer illiteracy, and high prices. Broadband internet, while widely available, remains prohibitively expensive for most of Egypt's population, nearly a fifth of which lives on less than US$2 a day.[3] There were only 1.1 million broadband subscribers in 2009,[4] although the actual number of users is hard to estimate because it is not unusual for users to share a connection, often illegally. Internet cafes offering such connections are common, even in urban slums and small villages.

The number of mobile-telephone users has grown to 55.3 million, constituting a 67 percent penetration rate.[5] Later generation mobile phones are available in the country. In April 2009, the government allowed the use of the Global Positioning System (GPS) feature, having previously banned it for security reasons.

A total of 214 internet-service providers (ISP)s serve Egypt's population of over 80 million. The largest ISP is TE Data, the communications and internet arm of state-owned landline monopoly Telecom Egypt. TE Data owns about 70 percent of internet bandwidth

[1] Egyptian Ministry of Communications and Information Technology, http://www.mcit.gov.eg, accessed July 3, 2010.
[2] International Telecommunications Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#, accessed February 20, 2011.
[3] World Bank, "Data—Indicators: Poverty Headcount Ratio at $2 a Day," http://data.worldbank.org/indicator/SI.POV.2DAY, accessed September 13, 2010.
[4] ITU, "ICT Statistics 2009—Internet"
[5] ITU, "ICT Statistics 2009—Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#, accessed February 20, 2011.

in Egypt. Three mobile-phone operators—Vodafone, Mobinil, and the Dubai-based Etisalat—serve Egyptian subscribers. All three offer broadband internet connections via USB modems. Mobile-phone services and ISPs are regulated by the National Telecommunication Regulatory Authority (NTRA), pursuant to the 2003 Telecommunications Regulation Law. As of the end of 2010, the NTRA's board was chaired by Minister of Communications and Information Technology Tarek Kamel, and included representatives from the presidency; the Ministries of Interior, Defense, Information, and Finance; the country's domestic intelligence service; and the State Security Council.[6] There were no reported incidents of ISPs being denied registration permits.

The video-sharing site YouTube; social-networking sites such as Facebook, MySpace, and Twitter; and various international blog-hosting services are freely available. Egypt is the leading Arab country in terms of Facebook use, with over 4.5 million users by the end of 2010.[7] There are nine radio stations broadcasting online in Egypt.[8] However, in March 2010, the NTRA banned access through USB modems to Skype, the voice over internet protocol (VoIP) application that allows users to make international phone calls via the internet. The service is still accessible through other types of internet connections.

LIMITS ON CONTENT

The government's sporadic efforts to remove websites that run against its interests and limit the spread of information through new technologies became first apparent in the run up to the November 2010 election. In the past, the authorities typically focused on intimidating users rather than actually removing content and blocking websites.[9] In fact, in December 2007, an administrative court judge issued a decision rejecting a request by a fellow member of the judiciary to ban 51 Egyptian websites, including those of several human rights organizations. In his decision, the judge emphasized the importance of respecting freedom of expression, including on the internet.[10]

Nonetheless, as political temperatures started to rise in the fall of 2010, several individuals who called for political change and democratic reform saw their websites affected. In one example, the blog belonging to Amr Osama—which promoted an opposition presidential candidate—was closed by its Emirati hosting service in September 2010. Those who later attempted to visit the site were greeted with a message by the

[6] National Telecommunication Regulatory Agency, "About Us: Board Members," http://www.tra.gov.eg/english/DPages_DPagesDetails.asp?ID=175&Menu=5, accessed July 10, 2010.
[7] CheckFacebook.com, "Egypt," http://www.checkfacebook.com/, accessed December 28, 2010.
[8] Naayem Saad Zaghloul, *Electronic Mass Communication in Egypt: Reality and Challenges* (Cairo: Egyptian Cabinet, Information and Decision Support Center, February 2010), 38.
[9] Rasha Abdulla, *The Internet in the Arab World: Egypt and Beyond* (New York: Peter Lang Inc., 2007).
[10] Arabic Network for Human Rights Information (ANHRI), "Court Rejects Request to Ban 51 Websites," International Freedom of Expression eXchange (IFEX), January 2, 2008, http://www.ifex.org/en/content/view/full/89371.

hosting service stating that the blog was removed due to a complaint by Gamal Mubarak, the president's son.[11] In another attempt to hamper the flow of independent news, in October, the NTRA issued a decision requiring that all group newsfeeds sent by short message service (SMS) had to be pre-approved by the regulator. The decision was a strong blow to independent civil society groups and media institutes who rely on mass messaging to disseminate news and information to their members; it was overturned by the State Council Administrative Court in November.

Also, in November, two Facebook groups, both popular platforms for organizing protests and with more than 200,000 members, were temporarily removed. One of the two groups "We Are All Khaled Said" emerged as the leading voice against police violence and corruption; the other group was in support of Mohammed ElBaradei, a former Director General of the International Atomic Energy Agency and a presidential hopeful favored by the opposition. Many suspect that the removals were carried out at the request of the Egyptian government, although Facebook claimed that the groups were removed because their administrators used pseudonymous accounts, which is in violation of the company's terms of use.[12]

The government maintains long-standing but unwritten "red lines" regarding certain sensitive issues, such as the president and his health; the military; Muslim-Christian tensions; Islam as a religion; and torture. Media personnel know that such topics should be handled with particular care, if at all. However, online activists and bloggers have become increasingly outspoken and routinely disregard most of these taboos. Internet users can freely access local and international political websites as well as the sites of human rights organizations, including some that harshly criticize the government and the political system.[13] In 2009, an administrative court ordered a ban on pornographic websites in Egypt, but the Ministry of Communications and Information Technology spoke against the court order, saying it is practically impossible as a technical matter to enforce an effective ban on pornography. The ban was never implemented.

In the past several years, Egypt has witnessed the birth of a lively and diverse blogosphere. Several bloggers have become media celebrities and won international awards for their work. Foremost among them is Wael Abbas, who received the prestigious Knight International Journalism Award in 2007. This in turn may have helped spur interest in internet activism among young Egyptians. The number of blogs was estimated at 160,000 in April 2008.[14] The popularity of the social networking site Facebook has also helped to create a culture of internet-based activism. Many bloggers now post "notes" and links to their blogs

[11]"Blog Shut Down After Promoting Opposition Candidate," IFEX, September 16, 2010 http://www.ifex.org/egypt/2010/09/16/amrosama.eb2a_blocked/.

[12] Danny O'Brien, "Facebook gets caught up in Egypt's media crackdown," Committee to Protect Journalists (CPJ), December 1, 2010, http://www.cpj.org/internet/2010/12/facebook-gets-caught-up-in-egypts-media-crackdown-1.php.

[13] Abdulla, *Policing the Internet in the Arab World* (Dubai: Emirates Center for Strategic Studies and Research, 2009).

[14] Zaghloul, *Electronic Mass Communication in Egypt*, 38.

on Facebook. Twitter is used to disseminate links to Facebook posts and blogs. Though Twitter is not yet very popular, messages posted to the service by ElBaradei have been widely read on Facebook.

As the number of blogs has increased, so has the diversity of opinion and content. In addition, opposition and human rights activists have found innovative ways to use blogs and social networking sites to call attention to causes and organize protests. In some cases, they have succeeded in doing what traditional activists could not. For example, in November 2007, a Cairo court sentenced two police officers to three years in prison for beating and raping a microbus driver based on video evidence that was first obtained by Abbas, who posted the material on YouTube.[15] The trial and sentencing of police officers for such wrongdoing was believed to be unprecedented. In 2008, a Facebook group formed by Esraa Abdel Fattah in support of workers in an Egyptian village called for a national day of strikes on April 6. The group gathered over 70,000 members and led to the formation of what is now known as the April 6 Youth Movement. The success of the group was aided by the fact that it caught the attention of the traditional media,[16] and thousands of Egyptians opted to stay home on the day of the strike. Internet also played an important role in protests, public discussions, and monitoring of the November 2010 elections. Since the government rejected the calls for international observers, a group of activists initiated a crowdsourcing and interactive mapping website based on the Ushahidi model, to quickly record and report on election violations.[17]

As of the end of 2010, the central goal for Egyptian internet activists and bloggers was political change. ElBaradei supporters and other activists were calling for Egyptians to sign a list of seven reform demands. They were hoping to pressure the government into abolishing the Emergency Law and enacting constitutional amendments that would limit presidents to two terms in office and make it possible for independents to run for the presidency.[18] They were also calling for the upcoming presidential election to be monitored by independent local and international observers to ensure fairness and transparency.

VIOLATIONS OF USER RIGHTS

No laws specifically grant the government the power to censor the internet. Egypt's constitution and the 2003 Law on Telecommunications uphold freedom of speech and

[15] Human Rights Watch, "Egypt: Police Officers Get Three Years for Beating, Raping Detainee," news release, November 6, 2007, http://www.hrw.org/en/news/2007/11/06/egypt-police-officers-get-three-years-beating-raping-detainee.
[16] Abdulla, *Policing the Internet in the Arab World*.
[17] "Activists Strive to Monitor Egyptian Vote," *Egyptian Gazette Online*, November 25, 2010, http://213.158.162.45/~egyptian/index.php?action=news&id=13154&title=Activists%20strive%20to%20monitor%20Egyptian%20vote.
[18] President Hosni Mubarak has been in power since 1981.

citizens' right to privacy, and require a judicial warrant for surveillance.[19] However, articles of the penal code and the Emergency Law—which has been in effect without interruption since 1981 and was most recently extended for another two years in 2010—give security agencies broad authority to monitor and censor all communications, and to arrest and detain individuals indefinitely without charge.[20] Amendments to the Press Law passed in 2006 preserved provisions that criminalize "spreading false news" and criticizing the head of state of Egypt or another country,[21] and courts have ruled that these restrictions apply to online writings.[22] Constitutional amendments passed in 2007 paved the way for future counterterrorism legislation that could make permanent the Emergency Law provisions allowing for widespread surveillance.[23] In 2010, Egypt saw the first court case in which a judge found an internet cafe owner liable for defamatory information posted online by a visitor to his shop.[24]

In 2008, Egypt proposed an Arab Satellite Broadcasting Charter to the information ministers of other Arab states at a meeting of the Arab League in Cairo. The nonbinding document, which is regarded as a serious threat to freedom of expression,[25] was adopted by most Arab countries, with the exceptions of Qatar and Lebanon. Egypt is working on a Satellite Broadcasting Regulation Law based on the charter, which would act as the regulatory document governing satellite and internet communications.

It is difficult to gauge the extent to which Egyptian security services monitor internet and mobile-phone communications, although a history of distrust between citizens and security forces has led to the widespread assumption that such monitoring could be in place at any time. All internet and mobile-phone users are required to register their personal information with the ISP or mobile operator. Those who buy a USB modem have to fill out a registration form and submit a copy of their national identification card. The same regulations apply for home internet subscribers. The government asks most internet cafes owners to record the names and identification numbers of their customers.

Social networking sites make it much easier for internet activists to organize, but they also allow government agents to monitor such activity and identify participants.[26] The government regularly applies offline punishments or intimidation to online activists.[27] This

[19] Law No. 10 of 2003, Article 65.
[20] Law No. 162 of 1958, renewed in 1981.
[21] Law No. 147 of 2006.
[22] "The Blogger and the Pharaoh," *International Herald Tribune*, February 26, 2007, http://www.iht.com/articles/2007/02/26/opinion/edblog.php.
[23] Amnesty International, "Egypt: Proposed Constitutional Amendments Greatest Erosion of Human Rights in 26 Years," news release, March 18, 2007, http://www.amnesty.org/en/library/info/MDE12/008/2007/en.
[24] "Journalist and Blogger Fined and Sentenced to Six Months in Jail," IFEX, September 3, 2010, http://www.ifex.org/egypt/2010/09/03/shehata_sentenced/.
[25] Article 19, "Arab Charter for Satellite TV: A Major Setback to Freedom of Expression in the Region," news release, February 13, 2008, http://www.article19.org/pdfs/press/egypt-adoption-of-the-arab-charter-for-satellite-tv.pdf.
[26] Abdulla, *Policing the Internet in the Arab World*.
[27] Ibid.

includes "friendly" warnings in phone calls from military or security officers, beating or detaining activists during street demonstrations, and court cases that may lead to prison sentences. In addition, security services use legal and extralegal means to collect users' internet and mobile-phone records from ISPs, internet cafes, and phone companies in the course of their investigations. These abuses have resulted in Egypt's inclusion on the Reporters Without Borders list of "internet enemies" since 2006, and as one of the 10 worst countries to be a blogger according to the Committee to Protect Journalists in 2009.[28]

Security services have used detentions and harassment, and in some cases torture, to intimidate online writers, and a growing number of bloggers have spent time in jail. In February 2007, Abd al-Karim Nabil Suleiman (widely known by his blogging name, Karim Amer), then a 22-year-old student of religious law at Al-Azhar University, became Egypt's first blogger to be sentenced to prison for his online writings. A court in Alexandria handed Suleiman a four-year prison term on charges of "inciting hatred of Islam" and "insulting the president."[29] He was released in November 2010.

Those who have been detained for shorter periods include Esraa Abdel Fattah, the creator of the Facebook group calling for the general strike on April 6, 2008. She was detained for two weeks that month on charges of "inciting unrest," but the charges were dropped by the prosecutor.[30] Also in 2008, Hany Nazeer was detained for a blog post that included a link to a book seen as insulting to Islam. He was kept in detention under the Emergency Law for 21 months before finally being released in July 2010.[31] In February 2010, blogger Ahmed Mostafa was detained and slated for trial before a military court, despite being a civilian, after he wrote about alleged abuses by the Egyptian army. The military abruptly dropped the case in March, however.[32] A Cairo appeals court in February reversed a lower court's November 2009 decision to sentence blogger Wael Abbas to six months in prison and a fine for allegedly damaging an internet cable, but in March an economic court gave him an identical sentence for providing telecommunications service without authorization.[33]

Internet activists have rallied around the case of Khaled Said, a 28-year-old who was allegedly beaten to death in June 2010 by two plainclothes policemen who dragged him

[28] Reporters Without Borders, "Internet Enemies: Egypt," March 12, 2010, http://en.rsf.org/internet-enemie-egypt,36679.html; Committee to Protect Journalists, "10 Worst Countries To Be a Blogger," special report, April 30, 2009, http://www.cpj.org/reports/2009/04/10-worst-countries-to-be-a-blogger.php.

[29] Reporters Without Borders, "Internet Enemies: Egypt."

[30] ANHRI, "Woman Detained for Promoting General Strike on Facebook, Released; Student Briefly Detained for Urging Release of Internet Activists," IFEX, April 24, 2008, http://www.ifex.org/egypt/2008/04/24/woman_detained_for_promoting_general/.

[31] John Ehab, "Controversial Blogger Released by Authorities," *Al-Masry al-Youm*, July 27, 2010, http://www.almasryalyoum.com/en/news/controversial-blogger-released-authorities.

[32] ANHRI, "Authorities Close Case Against Blogger Ahmed Mostafa," IFEX, March 11, 2010, http://www.ifex.org/egypt/2010/03/11/mostafa_case_closed/; ANHRI, "Blogger Tried in Military Court," IFEX, March 2, 2010, http://www.ifex.org/egypt/2010/03/02/mostafa_military_court/.

[33] Committee to Protect Journalists, "Egyptian Blogger Abbas, Cleared Once, Is Convicted Anew," news release, March 11, 2010, http://cpj.org/2010/03/egyptian-blogger-abbas-cleared-once-is-convicted-a.php.

from an internet cafe. The officers—now on trial for illegal arrest, torture, and excessive force, but not for murder—claimed that he choked to death while trying to swallow illegal drugs. He had reportedly posted a video on the internet showing policemen sharing the spoils of a drug bust, raising suspicions that he had been targeted for that reason.[34] A Facebook group called "We Are All Khalid Said" has garnered over 200,000 supporters (see also "Limits on Content"), and organized several offline demonstrations and protests, in which thousands of youths all over Egypt wore black and stood silently with their backs to the street.

In one of the most recent examples of government's misuse of power, Youssef Shabaan, a journalist for the online news outlet *Al-Badil,* was arrested in November 2010 while covering street protests in Alexandria and charged with drug possession. According to various independent groups, the charges against Shabaan were made up to punish him for his critical coverage of police brutality during the protests.[35]

[34] "Egypt Police in Brutality Trial over Khaled Said Death," British Broadcasting Corporation (BBC), July 27, 2010, http://www.bbc.co.uk/news/world-middle-east-10773404; Kareem Fahim, "Death in Police Encounter Stirs Calls for Change in Egypt," *New York Times*, July 18, 2010, http://www.nytimes.com/2010/07/19/world/middleeast/19abuse.html.
[35] "Egypt Detains Journalist on Drug Charges in Alexandria," Committee to Protect Journalists (CPJ), November 22, 2010, http://cpj.org/2010/11/egypt-detains-journalist-on-drug-charges-in-alexan.php.

ESTONIA

	2009	2011
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access	3	2
Limits on Content	2	2
Violations of User Rights	8	6
Total	**13**	**10**

POPULATION: 1.3 million
INTERNET PENETRATION: 72 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Free

INTRODUCTION

Estonia ranks among the most wired and technologically advanced countries in the world. However, when it regained independence in 1991 after nearly 50 years of Soviet rule, its infrastructure was in disastrous condition. President Toomas Hendrik Ilves remarked in 2008 that the Soviet legacy essentially necessitated Estonia's rapid technological development as it sought to integrate with the global economy.[1] The first internet connections in the country were introduced in 1992 at academic facilities in Tallinn and Tartu, and the government subsequently worked with private and academic entities to initiate a program called Tiger Leap, which aimed to computerize and establish internet connections in all Estonian schools by 2000. This program helped to build general competence and awareness about information and communication technologies (ICTs). Today, with a high level of computer literacy and connectivity already established, the focus has shifted from basic concerns such as access, quality, and cost of internet services to discussions about security, anonymity, the protection of private information, and citizens' rights on the internet. Local and international social-media services are used by more than 60 percent of internet users, and a majority of users conduct business and e-government transactions over the internet.[2]

The most serious threat to internet freedom in Estonia emerged in late April and early May 2007, when a campaign of cyberattacks targeted various Estonian institutions and

[1] "Estonia Became Internet Savvy 'Thanks' to Occupation—Ilves," Baltic News Service, April 15, 2008, available at http://www.estemb.org/news/aid-1549.
[2] Kristina Randver, "Kodanike rahulolu riigi poolt pakutavate avalike e-teenustega" [Citizens' Satisfaction with the Provision of Public E-Services], TNS Emor, May 11, 2010, available at http://www.riso.ee/et/files/Randver_infohommik_11.05.2010.pdf.

infrastructure. The experience led to increased awareness of the dangers of cyberattacks and a greater policy focus on improving technical competencies to make the internet more secure.

OBSTACLES TO ACCESS

The number of internet and mobile-telephone users in Estonia has grown rapidly in the past 15 years. According to 2009 estimates, the internet is regularly accessed by 72 percent of Estonia's population, or approximately 970,000 people.[3] There are also 2.7 million mobile-phone subscriptions—more than twice the number of people in Estonia. This outsized figure is commonly attributed to the growing popularity of machine-to-machine (M2M) services, widespread use of mobile internet-access devices, use of more than one mobile phone by individual Estonians, and the growing number of visitors who use local subscriptions while in the country.

The first public WiFi area was launched in 2001, and since then the country has developed a system of mobile data networks that enable widespread wireless broadband access. In 2009, the country had over 2,000 free, certified WiFi areas meant for public use, including cafes, hotels, hospitals, schools, and even gas stations, and the government has continued to invest in public WiFi. In addition, a countrywide wireless internet service based on CDMA technology has been deployed and priced to compete with fixed broadband access. Municipalities in rural areas have been subsidizing local wireless internet deployment efforts, and the country's regulatory framework presents low barriers to market entry, enabling local start-ups to proliferate.

Estonians use a large variety of internet applications, including search engines (85 percent of users), e-mail (83 percent), local online media, news portals, social-networking sites, instant messaging, and internet-based voice service.[4] In addition, 83 percent of the population uses the internet for online banking—the second highest percentage in the European Union.[5] Estonian Public Broadcasting delivers all radio channels in real time over the internet, and offers archives of its radio and television programs at no charge to users. YouTube, Facebook, LinkedIn, Orkut, and many other international video-sharing and social-networking sites are widely available and popular. According to December 2010 estimates, nearly 312,000 Estonians use Facebook, representing 23 percent of the overall

[3] International Telecommunication Union (ITU), "ICT Eye: Estonia," http://www.itu.int/ITU-D/ICTEYE/DisplayCountry.aspx?code=EST#jump, accessed August 11, 2010.

[4] Pille Pruulmann-Vengerfeldt, Margit Keller, and Kristina Reinsalu, "Quality of Life and Civic Involvement in Information Society," chap. 1.1.4 in *Information Society Yearbook 2009* (Tallinn: Ministry of Economic Affairs and Communications, 2010), http://www.riso.ee/en/pub/2009it/#p=1-1-4.

[5] "Estonians tend to avoid e-shopping—survey," Baltic News Service, February 8, 2008, available at http://www.estemb.org/news/aid-1247.

population.[6] Moreover, 21 percent of Estonians use the internet for uploading and sharing original content such as photographs, music, and text—the highest level of shared public communication in Europe.[7]

The Estonian Electronic Communications Act was passed in late 2004 to help develop and promote a free market and fair competition in electronic communications services.[8] Today there are over 200 operators offering such services, including six mobile-phone companies and numerous internet-service providers (ISPs). ISPs and other communications companies are required to register with the Estonian Technical Surveillance Authority (ETSA), a branch of the Ministry of Economic Affairs and Communications, though there is no registration fee.[9]

LIMITS ON CONTENT

Restrictions on internet content and communications in Estonia are among the lightest in the world. Nevertheless, due in part to Estonia's strong privacy laws, there are some instances of content removal. Most of these cases involve civil court orders to remove inappropriate or off-topic reader comments from news sites. Comments are similarly removed from online discussion forums and other sites. Generally, users are informed about a given website's privacy policy and rules for commenting, and they are expected to follow the instructions. In 2008, a debate over self-censoring and prepublication censorship took center stage when the victim of unflattering and largely anonymous comments attached to a news story filed suit, claiming that web portals must be held responsible for reader comments and screen them before they become public.[10] Website owners argued that they did not have the capacity to monitor and edit all comments made on their sites. Nonetheless, the Estonian courts ruled in favor of the plaintiff, making web portals responsible for all comments posted; the ruling was appealed to the European Court of Human Rights.

In January 2010, a new law on online gambling came into force, requiring all domestic and foreign gambling sites to obtain a special license or face access restrictions. As of July 2010, the Estonian Tax and Customs Board had placed 298 websites on its list of

[6] Socialbakers, "Estonia Facebook Statistics," http://www.facebakers.com/countries-with-facebook/EE, accessed December 26, 2010.
[7] Eurostat, "Individuals Using the Internet for Uploading Self-Created Content to Any Website to Be Shared," European Commission, http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00119, accessed June 10, 2010.
[8] Ministry of Economic Affairs and Communications, "Electronic Communications Act," http://www.mkm.ee/index.php?id=9576 , accessed March 26, 2009.
[9] Estonian Technical Surveillance Authority (ETSA), "Commencement of Provision of Communications Service," http://www.tja.ee/index.php?id=11703, accessed February 21, 2011.
[10] Kaja Koovit, "Big Businessman Goes to War Against Web Portals," Baltic Business News, March 18, 2008, http://www.balticbusinessnews.com/?PublicationId=48694078-50cc-4fe1-b3e4-6e10bc6a5ec1.

illegal online gambling sites, requiring Estonian ISPs to block them.[11]

There are over 54,000 active Estonian-language blogs on the internet, including an increasing number of group, project, and corporate blogs. The vibrancy and activities of the blogosphere are frequently covered by traditional media, particularly when blog discussions center on civic issues. The fact that so many Estonians are both computer literate and connected to the internet has created unique opportunities for the Estonian government. In addition to hosting virtual trade fairs and an online embassy, the Estonian president's office has its own YouTube channel, with messages released exclusively on YouTube.[12]

Estonia has the largest functioning public-key infrastructure in Europe, based on the use of electronic certificates maintained on the national identification (ID) card.[13] More than 1.12 million active ID cards are in use, which enable both electronic authentication and digital signing.[14] The law gives the digital signature the same weight as a handwritten one, and requires public authorities to accept digitally signed documents. Estonian ID cards were used to facilitate electronic voting during parliamentary elections in 2007, and they were used again in 2009 municipal and European Parliament elections. In 2009, over 91 percent of citizens filed their taxes over the internet, making the online services offered by the tax department the most popular public e-service. Over 63 percent of internet users regularly use e-government services, and 77 percent have indicated their satisfaction with such services.[15]

In April 2007, blogs and mobile-phone text messaging (SMS) played an important role in protests over the removal of a Soviet war monument. While it was known that the Estonian government was planning to remove the monument, no official announcement had been made. When the police cordoned off the area and covered the monument, word quickly spread via mobile phone and the internet, and within a few hours a crowd of several thousand had assembled.[16] Two days of rioting followed, mostly by ethnic Russians. However, as the physical violence receded, an unprecedented wave of cyberattacks against the Estonian government began. These "dedicated denial of service" (DDoS) attacks affected all of the government's websites, Estonia's largest bank, and the sites of several daily newspapers. Because of Estonia's level of connectivity, even simple activities like reading e-

[11] The list of restricted websites can be found on the Estonian Tax and Customs Board website: http://www.emta.ee/index.php?id=27399, accessed July 10, 2010.

[12] Agence France-Presse, "Estonia Launches Embassy in Virtual World Second Life," *Sydney Morning Herald*, December 5, 2007, http://www.smh.com.au/news/Technology/Estonia-launches-embassy-in-virtual-world-Second-Life/2007/12/05/1196530704693.html; "Estonian President Launches YouTube Video Blog," TopNews.in, December 9, 2008, http://www.topnews.in/estonian-president-launches-youtube-video-blog-297028.

[13] See the web portal for the ID-card system at http://id.ee/?lang=en.

[14] Ibid., accessed July 15, 2010.

[15] Kristina Randver, *Kodanike rahulolu riigi poolt pakutavate avalike e-teenustega, Jaanuary 2010* [Citizens' Satisfaction with the Provision of Public E-Services, January 2010] (Tallinn: TNS Emor, 2010), available at http://www.riso.ee/et/files/kodanike_rahulolu_avalike_eteenustega_2010.pdf.

[16] Veronica Khokhlova, "Estonia: 'A Russian Rebellion,'" Global Voices, April 27, 2007, http://globalvoicesonline.org/2007/04/27/estonia-a-russian-rebellion/.

mail and paying for a parking space were impossible. Officials were finally forced to block access to Estonian sites from IP addresses outside of Estonia in an effort to stop the attacks.[17] Throughout the three-week period of unrest, internet appeals and SMS messages continued to call for protests against the Estonian government.[18]

VIOLATIONS OF USER RIGHTS

Freedom of speech and freedom of expression are strongly protected by Estonia's constitution and by the country's obligations as a European Union (EU) member state. Anonymity is allowed, and there have been extensive public discussions on anonymity and the respectful use of the internet. Internet access at public access points can be obtained without prior registration. The Personal Data Protection Act (PDPA), first passed in 1996, restricts the collection and public dissemination of an individual's personal data. No personal information that is considered sensitive—such as political opinions, religious or philosophical beliefs, ethnic or racial origin, sexual behavior, health, or criminal convictions—can be processed without the consent of the individual. The Data Protection Inspectorate (DPI) is the supervisory authority for the PDPA, tasked with "state supervision of the processing of personal data, management of databases and access to public information."[19] The current version of the PDPA entered into force in 2008.[20]

There have been no physical attacks against bloggers or online journalists in Estonia, but online discussions are sometimes inflammatory. Following instances of online bullying and sexual harassment and misuse of social media, discussions and public-awareness campaigns were recently launched to raise parental involvement and increase protection of children on the internet.

Awareness of the importance of ICT security in both private and business use has increased significantly since the spring 2007 cyberattacks. To protect the country from future attacks, the government in 2008 adopted a Cyber Security Strategy for the next five years, which focuses on development and implementation of new security measures, increasing competence in cybersecurity, improvement of the legal framework, bolstering international cooperation, and raising public awareness.[21] Also in 2008, NATO established a joint cyberdefense center in Estonia to improve cyberdefense interoperability and provide

[17] "Estonia Hit by 'Moscow Cyber War,'" British Broadcasting Corporation (BBC), May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm.
[18] "Estonia Launches Probe into Internet Call for Armed Uprising," Agence France-Presse, May 3, 2007.
[19] Electronic Privacy Information Center (EPIC) and Privacy International, "Republic of Estonia," in *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (Washington: EPIC, 2007), available at http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-8.html.
[20] See the homepage of the Estonian Data Protection Inspectorate at http://www.aki.ee/eng.
[21] Cyber Security Strategy Committee, *Cyber Security Strategy* (Tallinn: Ministry of Defence, 2008), http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf.

cyberdefense support for all NATO members. Since its founding, the center has, among other activities, supported awareness campaigns and academic research on the topic, and hosted several high-profile conferences.[22]

[22] Cooperative Cyber Defence Centre of Excellence (CCD COE), "Conference on Cyber Conflict," http://www.ccdcoe.org/conference2010/, accessed July 15, 2010.

ETHIOPIA

	2009	2011
INTERNET FREEDOM STATUS	n/a	Not Free
Obstacles to Access	n/a	21
Limits on Content	n/a	26
Violations of User Rights	n/a	22
Total	n/a	69

POPULATION: 85 million
INTERNET PENETRATION: 0.5 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Although Ethiopia is one of Africa's most populous countries, poor infrastructure and a government monopoly on telecommunications have significantly hindered the expansion of digital media. As a result, Ethiopia has one of the lowest rates of internet and mobile-telephone penetration on the continent. Nevertheless, dissidents both inside the country and in the diaspora have increasingly used the internet as a platform for political discussion and criticism of the regime.

The government has responded by instituting one of the few nationwide filtering systems in Africa, passing laws to restrict free expression, and attempting to manipulate online media. These efforts have coincided with a broader increase in repression against independent print and broadcast media since the 2005 parliamentary elections, in which opposition parties mustered a relatively strong showing.[1] The crackdown gained new momentum ahead of the next elections in May 2010, though these were significantly less competitive. The ruling party and its partners obtained 544 of the 547 parliamentary seats and all but four of the 1,904 seats in regional councils, amid allegations of fraud and intimidation of opposition supporters.[2]

[1] Julia Crawford, "Ethiopia: Poison, Politics and the Press," Committee to Protect Journalists, April 28, 2006, http://cpj.org/reports/2006/04/ethiopia-da-spring-06.php.
[2] European Union Election Observation Mission to Ethiopia, *Ethiopia: Final Report, House of People's Representatives and State Council Elections, May 2010* (Brussels: European Union, 2010), http://www.eueom.eu/files/pressreleases/english/final-report-eueom-ethiopia-08112010_en.pdf.

Internet and mobile-phone services were introduced in Ethiopia in 1997 and 1999, respectively.[3] In recent years, the government has attempted to increase access through the establishment of fiber-optic cables, satellite links, and mobile broadband services. It has refused to end exclusive control over the market by the state-owned telecommunications firm, the Ethiopian Telecommunication Corporation (ETC). However, in December 2010 France Telecom took over management of ETC for a two-year period, renaming it Ethio Telecom in the process.[4] China has also emerged as a key investor and contractor in Ethiopia's telecommunications sector.[5] Given allegations that the Chinese authorities have provided the Ethiopian government with technologies that can be used for political repression, such as surveillance cameras and satellite jamming equipment,[6] some observers fear that the Chinese may assist the authorities in developing more robust internet and mobile-phone censorship and surveillance capacities in the coming years.

OBSTACLES TO ACCESS

Ethiopia's telecommunications infrastructure is among the least developed in Africa and is almost entirely absent from rural areas, which are home to about 85 percent of the population. In 2009, an estimated 915,000 fixed telephone lines were in operation, serving a population of 83 million, for a penetration rate of approximately 1 percent.[7] Similarly, as of 2009, there were only 447,000 internet users, for a penetration rate of 0.5 percent.[8] However, the number of actual subscriptions is lower, with a reported 74,600 fixed-line

[3] The first use of internet-like electronic communication was in 1993, when the United Nations Economic Commission for Africa (UNECA) launched the Pan African Documentation and Information Service Network (PADISNET) project, establishing electronic communication nodes in several countries, including Ethiopia. PADISNET provided the first store-and-forward e-mail and electronic-bulletin board services in Ethiopia. It was used by a few hundred people, primarily academics and staff of international agencies or nongovernmental organizations.

[4] William Davison, "France Telecom Takes Over Management of Ethiopia's Monopoly," Bloomberg, December 3, 2010, http://www.bloomberg.com/news/2010-12-03/france-telecom-starts-two-year-management-contract-at-ethiopia-s-utility.html.

[5] Isaac Idun-Arkhurst and James Laing, *The Impact of the Chinese Presence in Africa* (London: africapractice, 2007), http://www.davidandassociates.co.uk/davidandblog/newwork/China_in_Africa_5.pdf.

[6] Hilina Alemu, "INSA Installing Street Surveillance Cameras," *Addis Fortune*, March 21, 2010, http://www.addisfortune.com/Vol%2010%20No%20516%20Archive/INSA%20Installing%20Street%20Surrviellance%20Cameras.htm; "China Involved in ESAT Jamming," *Addis Neger*, June 22, 2010, http://addisnegeronline.com/2010/06/china-involved-in-esat-jamming/.

[7] International Telecommunications Union (ITU), "ICT Statisctics 2009—Fixed Telephone Lines," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/MainTelephoneLinesPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

[8] International Telecommunication Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#, accessed February 14, 2011.

internet connections in 2009, and only 3,500 of them broadband.[9] Mobile-phone penetration was roughly 5 percent, or about 4.1 million subscriptions, as of 2009.[10]

The combined cost of purchasing a computer, initiating an internet connection, and paying usage charges places internet access beyond the reach of most Ethiopians. The cost of mobile-phone broadband service ranges from a subscription charge of US$80 plus a monthly fee of US$255 for a 2.4 Mbps connection, to a subscription charge of US$10 plus a usage-based monthly fee for a 153.6 Kbps connection. For the second option, the actual speed is 70 to 80 Kbps, and an average subscriber using the connection mainly for e-mail and limited web functions would pay about US$20 per month.[11] By comparison, the gross domestic product per capita was US$318.70 in 2008.[12] A 2010 study by the International Telecommunication Union found that Ethiopia's broadband internet connections were among the most expensive in the world when compared with monthly income, second only to those in the Central African Republic.[13] Prices are set by ETC and kept artificially high; the Ethiopian government has been reluctant to liberalize the telecommunications sector, which would likely drive prices down. An adult literacy rate of 36 percent means that the majority of Ethiopians would be unable to take full advantage of online resources even if they had access to the technology.[14] Radio remains the principal mass medium through which most Ethiopians obtain information.

The majority of internet users rely on cybercafes to access the web, though connections there are often slow and unreliable. A 2010 study commissioned by Manchester University's School of Education found that accessing an online e-mail account and opening one message took six minutes in a typical Addis Ababa cybercafe with a broadband connection.[15] The number of cybercafes has grown in recent years, after a brief period in 2001–02 in which the government declared them illegal and forced some to shut down. Since July 2002, the Ethiopian Telecommunications Agency (ETA) has been authorized to issue licenses for new cybercafes.

The authorities have placed some restrictions on advanced internet applications. In particular, the use or provision of Voice over Internet Protocol (VoIP) services or internet-

[9] Ibid..
[10] ITU, "ICT Statistics 2009—Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#, accessed February 14, 2011.
[11] Ethio Telecom, "Detail Tariff for Leased Line Internet Through BBMN," http://www.ethionet.et/services/leasedlineinternetbbmntariff.html, accessed February 15, 2011.
[12] United Nations, "Country Profile: Ethiopia," *World Statistics Pocketbook*, http://data.un.org/CountryProfile.aspx?crName=Ethiopia, accessed August 26, 2010.
[13] Jonathan Fildes, "UN Reveals Global Disparity in Broadband Access," British Broadcasting Corporation (BBC), September 2, 2010, http://www.bbc.co.uk/news/technology-11162656.
[14] UNICEF, "Ethiopia: Statistics," http://www.unicef.org/infobycountry/ethiopia_statistics.html#67, accessed August 6, 2010.
[15] Andinet Teshome, *Internet Access in the Capital of Africa* (School of Education, University of Manchester, 2009), EthioTube video, 8:56, posted by "Kebena," http://www.ethiotube.net/video/9655/Internet-Access-in-the-Capital-of-Africa-Addis-Ababa, accessed August 06, 2010.

based fax services—including at cybercafes—is prohibited,[16] with potential punishments including a fine and up to five years in prison.[17] The government instituted the ban on VoIP in 2002 after it gained popularity as a less expensive means of communicating and began to drain revenue from the ETC's traditional telephone business.[18] Social-networking sites such as Facebook, the video-sharing site YouTube, and the Twitter microblogging service are available, though very slow internet speeds make it impossible to access video content. International blog-hosting websites such as Blogger have been frequently blocked since the disputed parliamentary elections of 2005, during which the opposition used online communication to organize and disseminate information that was critical of the ruling Ethiopian People's Revolutionary Democratic Front (EPRDF).[19] In addition, for two years following the 2005 elections, ETC blocked text-messaging via mobile phones after the ruling party accused the opposition of using the technology to organize antigovernment protests. Text-messaging services did not resume until September 2007.[20]

Ethiopia is connected to the international internet via satellite, a fiber-optic cable that passes through Sudan and connects to its international gateway, and another cable that connects through Djibouti to an international undersea cable.[21] In an effort to expand connectivity, the government has reportedly installed several thousand kilometers of fiber-optic cable throughout the country in recent years.[22] There are also plans in place to connect Ethiopia to a global undersea cable network through the East African Submarine Cable System (EASSy) project. The EASSy project itself was completed and launched in July 2010, but its effects on Ethiopia have yet to be seen.[23] The authorities have sought to increase access via satellite links for government offices and schools in rural areas. WoredaNet, for instance, connects over 500 woredas, or local districts, to regional and central government offices, providing services such as video conferencing and internet access. Similarly, SchoolNet connects over 500 high schools across the country to a gateway that provides video- and audio-streamed educational programming.[24] The impact of such projects has

[16] Ethiopian Telecommunication Agency (ETA), "Telecommunication Proclamation No. 281/2002, Article 2(11) and 2(12)," http://www.eta.gov.et/Scan/Telecom%20Proc%20281_2002%20(amendment)%20NG.pdf, accessed August 24, 2010.
[17] ETA, "Telecommunication Proclamation No. 49/1996, Articles 24 and 25," http://www.eta.gov.et/Scan/Telecom%20Proc%2049_1996%20NG1.pdf, accessed August 24, 2010.
[18] Groum Abate, "Internet Cafes Start Registering Users," *Capital*, December 25, 2006, http://www.capitalethiopia.com/index.php?option=com_content&view=article&id=259:internet-cafes-start-registering-users-&catid=12:local-news&Itemid=4.
[19] Bogdan Popa, "Google Blocked in Ethiopia," Softpedia, May 3, 2007, http://news.softpedia.com/news/Google-Blocked-In-Ethiopia-53799.shtml.
[20] Human Rights Watch, "Ethiopia: Repression Rising Ahead of May Elections," news release, March 24, 2010, http://www.hrw.org/en/news/2010/03/24/ethiopia-repression-rising-ahead-may-elections.
[21] Hailu Teklehaimanot, "Unraveling ZTE's Network," *Addis Fortune*, August 22, 2010, http://www.addisfortune.com/Interview-Unraveling%20ZTEs%20Network.htm.
[22] Samuel Kinde, "Internet in Ethiopia: Is Ethiopia Off-Line or Wired to the Rim?" MediaETHIOPIA, November 2007, http://www.mediaethiopia.com/Engineering/Internet_in_Ethiopia_November2007.htm.
[23] Brian Adero, "WIOCC-EASSy Cable Ready for Business," *IT News Africa*, July 23, 2010, http://www.itnewsafrica.com/?p=8419.
[24] Kinde, "Internet in Ethiopia."

been limited, however, as internet speeds across these networks remain almost prohibitively slow, and outages are common. In addition, as all of the networks are government owned and managed, the space for independent initiatives, entrepreneurial or otherwise, is extremely limited.[25] While a very small number of governmental and international organizations have their own VSAT satellite links to the internet with special government approval, such connections are not allowed for private organizations.[26]

The state-owned ETC, or Ethio Telecom, retains a monopoly on all telecommunications services, including internet access and both mobile and fixed-line telephony. Connection to the international internet is centralized via Ethio Telecom, from which cybercafes must purchase their bandwidth. The ETA is the primary regulatory body overseeing the telecommunications sector.[27] Although it was established as an autonomous federal agency, in practice it is tightly controlled by the government.

Liberalization of the telecommunications sector is expected to greatly increase internet and mobile-phone penetration, but the prospects for such liberalization remain uncertain. While some observers consider the December 2010 entry of France Telecom as manager of Ethio Telecom to be a potential move toward liberalization, others are skeptical of the government's commitment to allowing greater public access to information and communication technologies (ICTs). The foreign partnership may simply be an effort to improve service delivery while maintaining the state monopoly. The government has declared that it will not hasten the liberalization process or succumb to pressure from the international community.[28]

LIMITS ON CONTENT

Although the Ethiopian authorities deny engaging in online censorship,[29] studies conducted by the OpenNet Initiative (ONI) in 2009 indicate that Ethiopia is the only country in sub-Saharan Africa to impose nationwide, politically motivated internet filtering.[30] The blocking of websites is somewhat sporadic, tending to tighten ahead of sensitive political events. Following a period in early 2009 during which several previously blocked websites became

[25] Al Shiferaw, "Connecting Telecentres: An Ethiopian Perspective," *Telecentre Magazine*, September 2008, http://www.telecentremagazine.net/articles/article-details.asp?Title=Connecting-Telecentres:-An-Ethiopian-Perspective&articleid=163&typ=Features.

[26] Agencies including UNECA, the World Bank, and the Ethiopian Civil Service College have been given special authorization for a VSAT link.

[27] ETA, "Telecommunication Proclamation No. 49/1996, Part Two," http://www.eta.gov.et/Scan/Telecom%20Proc%2049_1996%20NG1.pdf, accessed August 24, 2010.

[28] Technology Strategies International, "ICT Investment Opportunities in Ethiopia—2010."

[29] "Ethiopia: Authorities Urged to Unblock Websites," Integrated Regional Information Networks (IRIN), May 25, 2006, http://www.irinnews.org/report.aspx?reportid=59115.

[30] OpenNet Initiative, "Regional Overview: Sub-Saharan Africa," http://opennet.net/research/regions/ssafrica, accessed May 28, 2010.

available, filtering intensified again ahead of the May 2010 elections as part of a general crackdown on independent and opposition media.[31]

The government's approach to internet filtering appears to entail hindering access to a list of specific internet-protocol (IP) addresses or domain names at the level of the international gateway. Testing by ONI found that the filtering focuses primarily on independent online news media, political blogs, and Ethiopian human rights groups' websites.[32] International news outlets such as the U.S.-based Cable News Network (CNN) and nongovernmental organizations such as Human Rights Watch, Amnesty International, and Reporters Without Borders—all of which have criticized the Ethiopian government's human rights record—were available as of early 2009. However, tests conducted by Freedom House found that in mid-2010 the websites of Freedom House, Human Rights Watch, and Amnesty International were inaccessible. In March 2010, Voice of America (VOA) reported that its website was blocked in Ethiopia.[33] This came shortly after Prime Minister Meles Zenawi admitted that the government was jamming VOA's Amharic radio service.[34] In addition, the British Broadcasting Corporation (BBC) reported in June 2010 that e-mail messages sent from Ethiopia to the U.S.-based Committee to Protect Journalists were being blocked.[35]

Ethiopian websites and blogs that are typically blocked but suddenly became available in early 2009 included CyberEthiopia, *Ethiopian Review*, Ethiopian Media Forum, Quatero, and Ethiomedia. Several observers suggested that the loosening came in response to the 2008 U.S. State Department human rights report on Ethiopia,[36] released in February 2009, which accused the government of restricting internet access by blocking politically oriented websites.[37] CyberEthiopia, a prodemocracy website, commented in March 2009 that the erratic nature of internet filtering may be a deliberate tactic by the authorities aimed at creating confusion and buttressing government claims that there is no systematic and pervasive filtering regime in the country. The article also raised concerns about a planned filtering system that would be capable of blocking access if blacklisted keywords are found at a given URL, but the existence of such a system has yet to be confirmed by additional

[31] Ben Rawlence, "100 Flowers of Repression Bloom as Ethiopia Moves to Gag Press Ahead of Elections," *East African*, April 12, 2010, available at http://www.hrw.org/en/news/2010/04/12/100-flowers-repression-bloom-ethiopia-moves-gag-press-ahead-elections.

[32] OpenNet Initiative, "Regional Overview: Sub-Saharan Africa."

[33] Barry Malone, "VOA Says Ethiopia Blocks Website as US Row Escalates," Reuters, March 29, 2010, http://af.reuters.com/article/topNews/idAFJOE62S0KX20100329?rpc=401&feedType=RSS&feedName=topNews&rpc=401&sp=true.

[34] "Ethiopia Admits Jamming VOA Radio Broadcasts in Amharic," BBC, March 19, 2010, http://news.bbc.co.uk/1/hi/world/africa/8575749.stm.

[35] Will Ross, "Donor Darling: What Ethiopian Poll Can Teach Africa," BBC, June 1, 2010, http://news.bbc.co.uk/1/hi/world/africa/10205887.stm.

[36] Bureau of Democracy, Human Rights, and Labor, "Ethiopia," in *2008 Country Reports on Human Rights Practices* (Washington, DC: U.S. Department of State, February 2009), http://www.state.gov/g/drl/rls/hrrpt/2008/af/119001.htm.

[37] Mohamed Keita, "Ethiopia Lifts Filtering of Critical Web Sites—At Least for Now," *Committee to Protect Journalists Blog*, March 4, 2009, http://cpj.org/blog/2009/03/ethiopia-lifts-filtering-of-critical-web-sites--at.php.

sources.[38] By mid-2010, all of the newly available websites and several others—including the online version of *Addis Neger*, a leading independent newspaper that was forced to close in December 2009[39]—were temporarily inaccessible again, apparently as part of the government's broader election-related restrictions on the free flow of information.[40]

The increased repression against journalists working in traditional media has generated a chilling effect in the online sphere. Few Ethiopian journalists work for both domestic print media and as correspondents for overseas online outlets, as this could draw negative repercussions. Many bloggers publish anonymously to avoid reprisals.

In addition to censorship, the authorities use regime apologists, paid commentators, and progovernment websites to proactively manipulate the online news and information landscape. Acrimonious exchanges between a small number of apologist websites and a wide array of diaspora critics and opposition forces have become common in the online Ethiopian political debate. In an example of alternative techniques for controlling online discussion, in April 2010 the *Addis Neger* prodemocracy Facebook group, which had attracted thousands of members, was shut down by Facebook administrators based on complaints that were apparently orchestrated by the regime; following international pressure, Facebook promptly reinstated the group.[41] Lack of adequate funding represents another challenge for independent online media, as fear of government pressure dissuades Ethiopian businesses from advertising with politically critical websites.

Regime critics and opposition forces in the diaspora increasingly use the internet as a platform for political debate and an indirect avenue for providing information to local newspapers. But given the low internet penetration rate, the domestic Ethiopian blogosphere is still in its infancy. Blogging initially blossomed during the period surrounding the 2005 parliamentary elections and the subsequent clampdown on independent newspapers. This growth has slowed somewhat since 2007, when the government instituted a blanket block on the domain names of two popular blog-hosting websites, Blogger and Nazret.com. Nevertheless, several bloggers, such as "Ethio-Zagol Seminawork" and "Urael," continued to use blogs to relay information abroad that exposed human rights violations, and to advocate for the release of political prisoners. Over the past two years, the use of social-networking sites, most notably Facebook, as platforms for political deliberation and information sharing has gained momentum, though many civil society groups based in the country are wary of mobilizing against the government. Some political commentators use

[38] "Ethiopia—Only Country in Sub-Saharan Africa to Actively Engage in Political Internet Filtering," CyberEthiopia, August 21, 2009, http://cyberethiopia.com/home/content/view/140/2/.
[39] Reporters Without Borders, "Weekly Forced to Stop Publishing, Its Journalists Flee Abroad," news release, December 4, 2009, http://en.rsf.org/ethiopia-weekly-forced-to-stop-publishing-04-12-2009,35258.html.
[40] Oromsis Adula, "Election 2010, Blogging, Medrek, and the Future of Ethiopia," Opride.com, http://www.opride.com/oromsis/ethiopia/647-election-2010-blogging-medrek-and-the-future-of-ethiopia.html, accessed May 25, 2010.
[41] "Facebook Urged to Reinstate Pro-Democracy Page," Ethiomedia, May 1, 2010, http://www.ethiomedia.com/absolute/3137.html.

proxy servers and anonymizing tools to hide their identity when publishing online and to circumvent filtering. Among general internet users, however, circumvention tools are rarely employed, and most people simply forego accessing websites that are blocked.[42]

VIOLATIONS OF USER RIGHTS

Constitutional provisions guarantee freedom of expression and media freedom.[43] Nevertheless, in recent years the government has adopted laws—namely the Mass Media and Freedom of Information Proclamation and the Anti-Terrorism Proclamation—that restrict free expression.[44] According to Human Rights Watch, the 2008 Mass Media and Freedom of Information Proclamation has some positive aspects, such as a ban on pretrial detention of journalists. However, it also introduced crippling fines, licensing restrictions for establishing a media outlet, a clause permitting only Ethiopian nationals to establish mass media outlets, and powers allowing the government to impound periodical publications.[45] The 2009 Anti-Terrorism Proclamation includes an overly broad definition of terrorism, leaving the authorities with wide discretion to invoke it when suppressing nonviolent dissent. Under the legislation, publication of a statement that is likely to be understood as a direct or indirect encouragement of terrorism is punishable by up to 20 years in prison.[46]

A criminal code that entered into force in May 2005 provides for "special criminal liability of the author, originator or publisher" when writings are deemed to be linked to offenses such as treason, espionage, or incitement; in such instances, the penalty may be life imprisonment or death.[47] Also under the criminal code, publication of a "false rumor" is punishable by up to three years in prison.[48] As of mid-2010, none of these laws had been used to prosecute an individual specifically for online expression, but the harsh legal regime has created a chilling effect on both traditional and online media.

Government surveillance of online and mobile-phone communications is a concern in Ethiopia, though there is a lack of concrete evidence as to the scale and scope of such

[42] Interview with an Ethiopian blogger and political commentator, August 8, 2010.
[43] "Constitution of the Federal Democratic Republic of Ethiopia, Article 29," Parliament of the Federal Democratic Republic of Ethiopia, http://www.ethiopar.net/, accessed August 24, 2010.
[44] Human Rights Watch, *Analysis of Ethiopia's Draft Anti-Terrorism Law* (New York: Human Rights Watch, 2009), http://www.hrw.org/en/news/2009/06/30/analysis-ethiopia-s-draft-anti-terrorism-law.
[45] "Freedom of the Mass Media and Access to Information Proclamation No. 590/2008," *Federal Negarit Gazeta* No. 64, December 4, 2008.
[46] "Anti-Terrorism Proclamation No. 652/2009," *Federal Negarit Gazeta* No. 57, August 28, 2009.
[47] International Labour Organization, "The Criminal Code of the Federal Democratic Republic of Ethiopia, Proclamation No. 414/2004, Article 44," http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/70993/75092/F1429731028/ETH70993.pdf, accessed August 24, 2010.
[48] International Labour Organization, "The Criminal Code of the Federal Democratic Republic of Ethiopia, Proclamation No. 414/2004, Articles 485 and 486," http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/70993/75092/F1429731028/ETH70993.pdf, accessed August 24, 2010.

practices. Upon purchasing a mobile phone, individuals are asked to register their SIM card with their full name, address, and government-issued identification number. Internet account holders also are required to register their personal details, including their home addresses, with the government. For a period following the 2005 elections, cybercafe owners were required to keep a register of their clients, but as of mid-2010 this was no longer being implemented in practice. The key government agency allegedly involved in surveillance is the Information Network Security Agency (INSA).[49] It is suspected of engaging in internet filtering and monitoring of e-mail.[50] There have also been reports of the government using technology obtained from the Chinese authorities to monitor phone lines and various types of online communication.[51]

Although traditional media journalists in Ethiopia face considerable harassment and intimidation, leading several to flee the country in recent years, there have been no reported cases of prosecution or attacks specifically in response to online expression or blogging.

[49] Information Network Security Agency of Ethiopia, "Mission Statement," http://www.insa.gov.et/INSA/faces/welcomeJSF.jsp, accessed June 2, 2010.
[50] Chris Forrester, "…While Ethiopia Starts Jamming," Rapid TV News, June 23, 2010, http://www.rapidtvnews.com/index.php/201006236926/while-ethiopia-starts-jamming.html.
[51] Helen Epstein, "Cruel Ethiopia," *New York Review of Books*, May 13, 2010, http://www.nybooks.com/articles/archives/2010/may/13/cruel-ethiopia/.

GEORGIA

	2009	2011
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access	15	12
Limits on Content	15	10
Violations of User Rights	13	13
Total	**43**	**35**

POPULATION: 4.6 million
INTERNET PENETRATION 2009: 30.5 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Use of the internet and related technologies continues to grow rapidly in Georgia, as does the availability of better connections and services. Social-networking sites, particularly Facebook, have gained in popularity in recent years,[1] reportedly eclipsing news sites and general web portals.[2] Facebook serves as an important platform for discussion and information exchange among the more liberal segments of Georgian society. State bodies have also been stepping up their use of the internet. For example, the National Agency of Public Registry (NAPR) allows citizens to register real estate through its website, and the tax inspection agency accepts online submission of tax declarations. The Ministry of Economy and Sustainable Development has reportedly turned its attention toward blogging and other social media.[3] There have been no recent reports of government restrictions on internet access or content.

The internet was first introduced in Georgia at the end of 1990s, and after a boom in new services like broadband at the beginning of 2004, connections became available for almost everyone with a telephone line in Tbilisi, the capital. Internet subscriptions have also proliferated in other large cities. Online news media are developing slowly, but a growing number of journals and newspapers are launching websites, and major newspapers and news agencies are sharing content through applications like Facebook, the Twitter microblogging

[1] Alexa, "Top Sites in Georgia," http://www.alexa.com/topsites/countries/GE, accessed September 20, 2010.
[2] Caucasus Research Resource Centers, "Georgian Media as Business: Data Snapshots," *Social Science in the Caucasus* (blog), December 11, 2009, http://crrc-caucasus.blogspot.com/2009/12/georgian-media-as-business-data.html.
[3] Georgian International Media Centre, "Blogging for Misha?" blog, April 14, 2010, http://georgiamediacentre.com/content/blogging_misha.

service, and the video-sharing site YouTube. Nevertheless, many journalists working in traditional media lack knowledge about internet technology and web tools.

OBSTACLES TO ACCESS

The number of internet and mobile-telephone users is growing, but high prices for services and inadequate infrastructure remain obstacles to access, particularly for those in rural areas or with low incomes. According to the International Telecommunication Union, Georgia had 1.3 million internet users in 2009, which constitutes a 30.5 percent penetration rate.[4] Internet-service providers (ISPs) offer dial-up, DSL broadband, fiber optic, and wireless connections. As of the end of 2009, there were 150,000 broadband subscriptions in Georgia.[5] The average cost for an internet connection is US$25 a month. The lowest price for a 1 Mbps broadband connection is about US$10.

Mobile-phone penetration is deeper than that of the internet, with a total of 2.8 million subscribers in 2009, out of a population of 4.3 million.[6] This represents a notable increase since 2004, when there were only 840,000 subscriptions. Mobile phones significantly outnumber landlines, and reception is available throughout the country, including rural areas. The use of mobile phones to connect to the internet has been limited by high costs, but providers are offering new and somewhat less expensive services, and usage is growing.

Most Georgian users, about 55 percent, access the internet from home, while about 21 percent use a friend's computer. Others use connections at the office (9 percent), on mobile phones (6 percent), or in cybercafes (6 percent).[7] Cybercafes provide internet access for reasonable fees, but they are located mainly in large cities and there are too few to meet the needs of the population. Most cafes have less than a dozen computers, and customers often have to wait as long as an hour for access. Many restaurants, cafes, bars, cinemas, and other gathering places provide WiFi access, allowing customers to use the internet on their personal laptops.

There are 19 ISPs in Georgia, though two of them serve more than two-thirds of the market: Silknet (formerly United Telecom of Georgia, or UTG) with more than 40 percent and Caucasus Online with a somewhat smaller share. Three of the 19 are mobile operators.[8]

The telecommunications infrastructure in Georgia is still weak, and users may find that two or three times per month, only Georgian sites are accessible and no international

[4] International Telecommunication Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx.
[5] Ibid.
[6] ITU, "ICT Statistics 2009—Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx.
[7] Caucasus Research Resource Centers, "Georgian Media as Business: Data Snapshots."
[8] This data was obtained in September 2010. For current data, see Top.ge at http://top.ge/all_report.php.

connection is functional. Caucasus Online is most commonly affected by this phenomenon. The ISP provides no explanation of why the problem occurs or how it can be solved. Experts often cite breakdowns related to an underwater cable in the Black Sea. In general, the connection speed for accessing content hosted in Georgia is greater than for international content.

The Georgian National Communications Commission (GNCC) is the main media regulatory body, and although there have yet to be many test cases, it seems to be fair in dealing with internet companies. However, there is no significant difference between GNCC procedures for handling traditional media and those pertinent to telecommunications and internet issues, so criticism surrounding the commission's alleged lack of transparency and flawed licensing procedures for traditional media may reappear in the context of internet regulation.

LIMITS ON CONTENT

Government censorship is not a major hindrance to internet freedom in Georgia. Users can freely visit any website around the world, upload or download any content, and contact other users via forums, social-networking sites, and applications like instant messaging. In fact, content is so accessible that numerous sites offer illegal material such as pirated software, music, and movies, and the government has not enacted appropriate legal measures to combat the problem. ISPs still own websites with a great deal of pirated material,[9] but visits to such sites have decreased and given way to social-networking, video-sharing, blogging, and news sites.[10] Within some state institutions and private companies there is a small degree of censorship designed to improve worker productivity and limit internet traffic, for example by blocking access to Facebook and YouTube. At the same time, both governmental bodies and private employers are increasingly using social media for recruitment and public-relations purposes.

While the authorities do not regularly block public access to specific websites, there have been a few cases in which they interfered with internet access on a large scale. In August 2008, during a brief military conflict between Georgia and Russia, the government blocked access to all Russian addresses (those using the .ru country code) in an effort to prevent users from receiving "unofficial" information about the fighting. The move was also a response to attacks launched by Russian hackers against Georgian government websites. In addition to limiting access to certain news content, the government's actions affected Georgian users' ability to reach advanced applications based in Russia, including the popular

[9] See, for example, http://gol.ge/; http://avoe.ge/movies/.
[10] Alexa, "Top Sites in Georgia."

blogging service LiveJournal. The filtering was eased within days, and currently no such restrictions are in force.

There is no law that specifically regulates internet censorship or bans inappropriate content, such as pornography or violent material. The Law of Georgia on the Protection of Minors from Harmful Influence addresses gambling and violence, but it does not refer to online activities.[11] Nevertheless, this legal ambiguity could be exploited to impose significant internet content restrictions in the future.

YouTube, Facebook, and international blog-hosting services are freely available. Indeed, Facebook is now the most popular site on the Georgian internet. A number of bloggers and journalists use it to share or promote their content, gaining readers and starting discussions on current events. However, one recent event prompted some concern among internet activists. In April 2010, the administrator of the Facebook group "Against Nanukas Show," which was critical of the hostess of the Nanukas television talk show, alleged that he was threatened by unidentified state employees and forced to make the group inactive.

Inadequate revenues in the online news business, combined with a lack of technological knowledge, has hampered the expansion of traditional media outlets to the internet. The government's apparent interest in blogging and social media could help spur traditional outlets to establish a greater internet presence, but this would also require more private investment in online advertising. At present, most online media outlets face difficulty in attracting advertisers, but the problem seems to be more acute for the sites that are critical of the government. Some media owners reported instances in which advertisers decided to withdraw ads from websites after those outlets published news articles overly critical of the government or the ruling party.

There are about 100 bloggers writing in the Georgian language who try to remain active and current. However, at this point the blogosphere is still very weak. Minorities are not restricted from internet use, but they are represented online through only a small number of forums and blogs. Similarly, there is little representation of other vulnerable groups, such as internally displaced persons from conflict regions like South Ossetia. Although most Georgians use the Internet as a source of entertainment, various Web.2.0 applications have become an important platform for discussion and information exchange. In one example, an employee of the Interior Ministry was fired after he was identified by Facebook users as the person who punched a female opposition activist during anti-government protests.[12]

[11] The law is available in English on the GNCC website at http://www.gncc.ge/index.php?lang_id=ENG&sec_id=7050&info_id=6521.

[12] Mirian Jugheli "Georgia: Policeman Fired After Being Identified on Facebook," The Young Georgians, January 7, 2011, http://theyounggeorgians.wordpress.com/2011/01/07/georgia-policeman-fired-after-being-identified-on-facebook/.

VIOLATIONS OF USER RIGHTS

Civil rights including the right to access information and freedom of expression are guaranteed by the Georgian constitution,[13] and they are generally respected in practice. Article 20 of the constitution and Article 8 of the Law of Georgia on Electronic Communications include privacy guarantees for users and their information, but they simultaneously allow privacy rights to be restricted by the courts or other legislation.[14] The Law on Freedom of Speech and Expression "makes it clear that other 'generally accepted rights' related to freedom of expression are also protected even if they are not specifically mentioned."[15] Nonetheless, internet activities can be prosecuted under that law—mainly in cases of alleged defamation—or under any applicable criminal law.

In November 2009, two young students were detained after allegedly insulting the widely respected head of the Georgian Orthodox Church in videos that were posted on YouTube.[16] This remains the only known case in which law enforcement officials acted in response to internet-based discussion of controversial content (on Facebook and forum.ge), although the issue was also taken up by traditional media. Without conducting a formal criminal investigation, police detained the two youths, confiscated their computers and other hardware, and forced them to take down the parody videos before releasing them. The confiscated hardware was not returned, and the legal basis for these actions was not explained.

Georgian legislation grants police and security services significant discretion in conducting surveillance. Police can generally begin surveillance without a court's approval, though they must obtain it within 24 hours. There are some official requirements for launching such monitoring, but in reality it is sufficient to label the targeted individual a suspect or assert that he may have criminal connections. New amendments to the Law on the Operative-Investigative Activity, promulgated in September 2010, require that websites, mail servers, internet service providers, and other relevant companies make available private communications such as emails and chats to law enforcement authorities,

[13] The constitution is available in English at http://www.parliament.ge/index.php?lang_id=ENG&sec_id=68.
[14] The law is available in English on the GNCC website at http://www.gncc.ge/index.php?lang_id=ENG&sec_id=7050&info_id=3555.
[15] Article 19, *Guide to the Law of Georgia on Freedom of Speech and Expression* (London: Article 19, April 2005), http://www.article19.org/pdfs/analysis/georgia-foe-guide-april-2005.pdf.
[16] "Police Say Identified Patriarch Mocking Video Producers," Civil Georgia, November 1, 2009, http://civil.ge/eng/article.php?id=21629&search=buasili; Molly Corso, "Georgia: Free-Speech Debate Swirls in Tbilisi Over Patriarch Parody," Georgian Daily, November 2, 2009, http://georgiandaily.com/index.php?option=com_content&task=view&id=15482&Itemid=134&lang=en; Georgian International Media Centre, "Saakashvili Brings Internet Censorship to Georgia after Embarrassment over Patriarch Videos," blog, November 1, 2009, http://georgiamediacentre.com/content/saakashvili_brings_internet_censorship_georgia_after_embarrassment_over_patriarch_videos.

provided that a court approval is obtained.[17] It is yet to be seen how the new law will be implemented in practice.

Additionally, ISPs are obliged to deliver statistical data—separated by user—about site visits, traffic, and other topics. Mobile-phone companies are required to provide similar data when asked by the government. Cybercafes are not obliged to comply with government monitoring, as they do not register or otherwise gather data about customers. Individuals are not required to register when they buy a mobile phone, but registration is needed to buy a SIM card and obtain a number.

While cyberattacks are not very common in Georgia, they do occur and are often related to political tensions between Georgia and Russia. For example, Russian hackers conducted large-scale attacks on Georgian government sites during the August 2008 conflict. The websites of the parliament and the Ministry of Foreign Affairs were knocked out for a few days, with defamatory images of the Georgian president posted in their place. More recently, in August 2009, a Georgian blogger known as Cyxymu was the target of a denial-of-service attack that ultimately affected hundreds of millions of users worldwide and caused disruptions in the functioning of Facebook, Twitter, and the popular blog-hosting site LiveJournal. The blogger, a critic of Russia's conduct in the disputed territory of South Ossetia, blamed the Kremlin for the attack.[18]

[17]Tamar Chkheidze, "Internet Control in Georgia," Humanrights.ge, November 17, 2010, http://www.humanrights.ge/index.php?a=main&pid=12564&lang=eng.

[18] Tom Parfitt, "Georgian Blogger Cyxymu Blames Russia for Cyber Attack," *Guardian*, August 7, 2009, http://www.guardian.co.uk/world/2009/aug/07/georgian-blogger-accuses-russia.

GERMANY

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Free**
Obstacles to Access	n/a	4
Limits on Content	n/a	5
Violations of User Rights	n/a	7
Total	**n/a**	**16**

POPULATION: 81.6 million
INTERNET PENETRATION: 72 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Free

INTRODUCTION

Telecommunications in Germany are an increasingly contested arena in which the state, civil society leaders, and powerful private companies including internet-service providers (ISPs) assert sometimes incompatible rights and interests. There is a great deal of legal uncertainty in two key areas of internet freedom: a data-retention law has been ruled unconstitutional, and controversy surrounding a new law for blocking internet content has prevented it from being applied to date. Furthermore, while the constitution contains strong privacy protections, and private companies that violate them have been held accountable, lawmakers have increasingly curbed privacy rights in certain contexts, particularly with respect to government-approved surveillance. On other issues, such as the liability of ISPs for content, conflicting court decisions have added to legal ambiguity.

OBSTACLES TO ACCESS

The infrastructure is well developed, with electricity and at least fixed-line telephony in all homes. Mobile-telephone access is ubiquitous. In 2009, there were a total of 108 million mobile subscriptions in Germany, compared with 82.7 million inhabitants.[1] In terms of internet access, 72 percent of the population over 14 years old were considered users in

[1] See BuddeComm, "Germany—Mobile Market: Statistics and Forecasts," https://www.budde.com.au/Research/Germany-Mobile-Market-Overview-Statistics-Forecasts.html, accessed September 2, 2010. For the development of mobile-phone access in Germany since 1990, see Bundesnetzagentur [Federal Network Agency], *Annual Report 2009* (Berlin: Bundesnetzagentur, 2010), 90, available at http://www.bundesnetzagentur.de/cln_1931/EN/PressSection/Publications/publications_node.html.

2009–2010. Broadband service, defined as a connection speed of at least 1 Mbps, is almost universally available.[2] However, in 2010 only 49.6 percent of the population actually used broadband service.[3]

Private ownership of computers and home internet connections are the norm. The 1990s privatization of the telecommunications sector in Germany has led to a stark drop in prices.[4] Current flat rates for internet service are below €24 (US$30) per month.[5] In addition, users can take advantage of free access at public institutions like libraries. Nevertheless, a sizeable share of the population makes little or no use of computers or the internet, whether out of lack of interest or lack of computer literacy.

Thanks to school-related access, 97.5 percent of all students aged 14 to 19 are internet users. Underprivileged groups are less likely to use the internet; they include women, older people, people with less formal education and less income, residents of the eastern states (formerly under communist rule) or very small cities, and people living alone.[6] Only 26 percent of the population uses the internet routinely and in a substantial way, and members of this group are typically male and 36 years old or younger.[7]

The video-sharing site YouTube, the Facebook social-networking site, the microblogging service Twitter, and international blog-hosting platforms are freely available. However, the four mobile-telephony providers in Germany prohibit in their general terms and conditions internet-based services, such as Voice over Internet Protocol (VoIP) and instant messaging, that would threaten their revenue from the equivalent telephony-based services. While these prohibitions have apparently not been enforced, their legality is questionable.[8] Similarly, the private ISP Kabel Deutschland was found in 2008 to have slowed down its connections during certain times of the day, which adversely affected users of the video-sharing technology BitTorrent in particular.[9] Such practices raise questions about the protection of net neutrality, which is coupled with the protection of telecommunications secrecy laid down in Section 88 of the Telecommunications Act.

The privatization of the telecommunications sector was undertaken with the aim of fostering competition. However, the market has become concentrated in the hands of a few

[2] Bundesministerium für Wirtschaft und Technologie [Federal Ministry of Economics and Technology, BMWi], *Breitbandatlas 2009_2* (Berlin: BMWi, 2009), 7, available at: http://www.zukunft-breitband.de/BBA/Navigation/Service/publikationen,did=303750.html (in German).
[3] Initiative D21, *(N)Onliner Atlas 2010* (Berlin: Initiative D21, 2010), 10, available at http://www.initiative21.de/category/nonliner-atlas/nonliner-atlas-2010 (in German).
[4] Bundesnetzagentur, *Annual Report 2009*.
[5] See, for instance, http://telko.check24.de or http://www.dslweb.de.
[6] Initiative D21, *(N)Onliner Atlas 2010*, 42.
[7] Initiative D21, *Digitale Gesellschaft: Die digitale Gesellschaft in Deutschland—Sechs Nutzertypen im Vergleich* (Berlin: Initiative D21, 2010), http://www.initiative21.de/wp-content/uploads/2010/03/Digitale-Gesellschaft_Endfassung.pdf (in German).
[8] Christoph H. Hochstätter, "Lauschangriff DPI: So hören die Provider ihre Kunden ab," ZDNet.de, March 24, 2009, http://www.zdnet.de/sicherheits_analysen_lauschangriff_dpi_so_hoeren_die_provider_ihre_kunden_ab_story-39001544-41001975-1.htm (in German).
[9] Janko Röttgers, "Internetanbieter bremst Taschbörsen aus," Focus Online, March 6, 2008, http://www.focus.de/digital/internet/kabel-deutschland_aid_264070.html (in German).

large companies over the past decade. The emerging leaders among ISPs and backbone internet providers are Deutsche Telekom, Arcor, United Internet, Freenet, QSC, Versatel, Telefónica, and AOL; many small ISPs have been forced out of business.[10] The country's four large mobile-phone companies are T-Mobile, E-Plus Mobilfunk, Telefónica O2, and Vodafone D2. Internet cafes are common in Germany, though their number may be decreasing amid growing individual computer ownership and the free wireless connections now offered in many bars and cafes. The main regulatory burdens faced by internet cafes relate to the protection of youth from harmful content and practices.[11]

ISPs must meet the technological and administrative requirements laid out in a decree on telecommunications interception before they can start doing business.[12] The entity responsible for regulating digital technology is the Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railway (Bundesnetzagentur), operating under the auspices of the Federal Ministry of Economics and Technology. Its decisions, which are based on the Telecommunications Act, may be challenged directly before the administrative courts. Section 5(1) of the Federal Network Agency Act provides for an Advisory Council consisting of 16 members of the lower house of parliament and 16 representatives of the upper house, appointed by the federal government on the parliament's recommendation. The Advisory Council focuses on issues surrounding spectrum management, frequency usage, universal service obligations, and strategic policies of market relevance. [13] It also submits proposals to the federal government concerning the appointment of the president and the two vice presidents of the Federal Network Agency, who serve five-year terms and may be reappointed. They may also be dismissed if there is a serious reason to do so. The German Monopoly Commission has voiced the concern that this leaves the agency vulnerable to "political instrumentalization."[14] Separately, in 2010, the European Commission criticized the Federal Network Agency for passivity and the drawn-out nature of its regulatory procedures, which in practice might give a competitive

[10] See, for instance, the websites www.providersuche.org and www.teltarif.de/i/backbone.html.

[11] These mainly relate to online content, gaming, and the availability of alcohol in internet cafes. See Bundesprüfstelle für jugendgefährdende Medien [Federal Department for Media Harmful to Young Persons, BPjM], "Internetcafés: Rechtsauffassung der obersten Landesjugendbehörde zur jugendschutzrechtlichen Einordnung von gewerblichen Internetcafés," in *BPJM Aktuell 4* (Berlin: BPjM, 2005), http://www.bundespruefstelle.de/bpjm/redaktion/PDF-Anlagen/bpjm-aktuell-internetcafes-rechtsauffassung-der-oljb-aus-04-05,property=pdf,bereich=bpjm,sprache=de,rwb=true.pdf (in German).

[12] The decree's full title is "Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation." It is available at http://www.gesetze-im-internet.de/bundesrecht/tk_v_2005/gesamt.pdf (in German).

[13] Bundesnetzagentur, "Advisory Council," http://www.bundesnetzagentur.de/cln_1912/EN/FederalAgency/AdvisoryCouncil/advisorycouncil_node.html, accessed September 7, 2010.

[14] Monopolkommission [Monopoly Commission], *Telekommunication 2009: Klaren Wettbewerbskurs halten* (Berlin: Monopolkommission, 2009), 75, http://www.monopolkommission.de/sg_56/s56_volltext.pdf (in German). The European Commission has also taken up this concern. See European Commission, *Progress Report on the Single European Electronic Communications Market, 15th Report* {COM(2010) 253}, 196, http://ec.europa.eu/information_society/policy/ecomm/doc/implementation_enforcement/annualreports/15threport/15report_part1.pdf.

advantage to Deutsche Telekom, the former state-owned monopoly.[15]

LIMITS ON CONTENT

The penal code contains provisions against certain types of public speech, most notably the propaganda of unconstitutional organizations (Section 86); hate speech, defamation, and calls for violence against segments of the population (Section 130); utterances that deny or render harmless acts committed under the rule of National Socialism and are capable of disturbing the public peace (Section 130); instructions for serious crimes (Section 130a); representations of violence against human beings that appear to glorify such violence or render it harmless, or that injure human dignity (Section 131); and pornography focused on acts of violence or sexual acts of human beings with animals (Section 184a) or with children under age 14 (Section 184b). Pornography in general is not forbidden, but it is illegal to give juveniles under age 18 access to it or facilitate their access to it (Section 184[1] and [2]). There are also laws prohibiting defamation, the divulging of state secrets, copyright violations, fraud (including phishing), spam, malware, and viruses.

Blocking is employed when illegal content is hosted abroad and entities in the host country are unwilling to remove it. While there is effective international collaboration on content removal with respect to problems like fraud,[16] extreme right-wing and neo-Nazi content is illegal in Germany but not in many other countries where it is hosted, meaning such material must be blocked in Germany.[17]

A new law restricting child pornography, signed in February 2010, has generated heated public debate. The measure requires ISPs to block access to pages containing child pornography, and authorizes the Federal Criminal Office (BKA) to compile continuously updated lists of the sites to be blocked. The law, which will only be in effect until the end of 2012, contains many legally questionable components, and has already fallen into so much disfavor that courts will reportedly not take it into consideration.[18] When the law was being drafted, a huge public campaign coordinated in large part by the Working Group Against Internet Blocks and Censorship recommended takedown notices and prosecution rather than blocking as an appropriate remedy.

[15] European Commission, *Progress Report*, 196.

[16] Tyler Moore and Richard Clayton, *The Impact of Incentives on Notice and Take-down* (Cambridge, UK: University of Cambridge, 2008), http://www.cl.cam.ac.uk/~rnc1/takedown.pdf.

[17] The blocking is hard to quantify, as there appears to be a great deal of fluctuation, with hundreds of extreme right-wing sites being blocked or taken down and hundreds of new ones surfacing each year. In 2007, for example, there were reportedly 250 new right-wing internet sites, and roughly the same number were deleted from the internet. Agence France-Presse, "SPD: Sperrung von 231 Internetseiten in öffentlichen Gebäuden," Focus Online, December 9, 2008, http://www.focus.de/politik/deutschland/spd-sperrung-von-231-internetseiten-in-oeffentlichen-gebaeuden_aid_354643.html (in German).

[18] Uwe Hessler, "German Child Pornography Law Hits Snags," Deutsche Welle, February 23, 2010, http://www.dw-world.de/dw/article/0,,5278471,00.html.

The role given to the BKA by the law was also criticized, with opponents arguing that content issues should be dealt with at the state level. Existing federal laws, such as the Telemedia Act and the Telecommunications Act, address general liability, data protection, and information transport, not content. Moreover, the BKA list is not open to the public and the procedures for checking its accuracy and challenging it directly appear inadequate. An independent expert group is tasked with drawing random samples from the list to determine whether the content is indeed child pornography. To appeal a listing, the website owner would have to go to administrative court.

Although there is a federal law addressing youth protection in different types of media, youth protection on the Internet is principally addressed by the states and their joint agreement on the topic, known as the Jugendmedienschutz-Staatsvertrag (JMStV).[19] Compliance with the JMStV, which outlaws content similar to that outlawed by the penal code, is overseen by the Commission for Youth Protection Relating to Media, which can ask the Federal Department for Media Harmful to Young Persons to put a website on its blacklist of youth-endangering media. Offending website owners residing in Germany are prosecuted, but if they are beyond the reach of German authorities, the blacklist is made available for integration into privately owned filtering software. Moreover, service providers have formed a voluntary self-regulation entity called the Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM), and participating search-engine companies have agreed to remove blacklisted websites from their search results.[20] Content that is forbidden to children but not to adults, such as adult pornography, must be made available in a way that verifies the age of the user.[21]

There is no censorship prior to publication. However, figures released by Google in 2010 on the number of requests for postpublication content removal by government entities seem to indicate that this strategy is used extensively in Germany. The country ranked second, behind Brazil, with 188 requests for removal between July 1, 2009, and December 31, 2009. Google complied fully or partially with 94.1 percent of these requests.[22] Notably,

[19] A revision of the JMStV was due to be adopted by the end of 2010, but eventually failed. It would have required each website hosted in Germany to include a tag like a movie rating specifying if its content should be restricted to certain age groups (e.g. six years and older, 12, 16 or 18 years and older). Critics of this revision conducted an experiment showing that even ratings specialists did not agree when trying to rate internet content, let alone any number of private individuals, who would under the new JMStV have to rate their own material. Further unresolved issues concerning this rating included liability and supervision issues and how to even apply such a provision to dynamic websites. See "Jugendmedienschutz-Novellierung endgültig gescheitert," *Heise Online* December 16, 2010, http://www.heise.de/newsticker/meldung/Jugendmedienschutz-Novellierung-endgueltig-gescheitert-1154880.html (in German).

[20] Currently, Google search results state how many hits have been removed for legal reasons, and offer a link to ChillingEffects.org for more information. Users who follow this link have to opportunity to compare the results for their search between Google.de and Google.com.

[21] BPjM, *BPJMThema Wegweiser Jugendmedienschutz: Ein Überblick über Aufgaben und Zuständigkeiten der Jugendmedienschutzinstitutionen in Deutschland* (Berlin: BPjM, 2009), http://www.bundespruefstelle.de/bpjm/redaktion/PDF-Anlagen/bpjm-thema-wegweiser-jugendmedienschutz,property=pdf,bereich=bpjm,sprache=de,rwb=true.pdf (in German).

[22] Google, "Transparency Report: Government Requests," http://www.google.com/governmentrequests/, accessed September 7, 2010.

other European countries logged far fewer requests; the only ones with more than 10 were Britain (59), Italy (57), and Spain (32). According to the German news website *Spiegel Online*, the content at issue in the German requests was mainly defamation, Holocaust denial, and unconstitutional neo-Nazi material.[23] The Google figures do not include sites removed because of child pornography or copyright infringements, or removals that Google initiated based on its own policies, such as a rule against hate speech on its blog-hosting platform, Blogger.[24]

Paragraph 8 of the Telemedia Act expressly states that access providers are not legally responsible for their customers' content unless they collaborate with users in breaking the law. However, courts have continued to disagree on whether web-hosting businesses and access providers can be made liable under the concept of *Störerhaftung* (liability of the interferer), defined in the civil code (for example in Sections 862 and 1004) as interference with the property of others. This concept has been invoked with respect to intellectual-property rights, business competition, and personality rights, among other topics.

A 2009 decision by a state court in Hamburg controversially extended the concept of *Störerhaftung* from web-hosting services to access providers. The access provider Hansenet/Alice had asked the court whether it was obliged to block access to websites with illegal content. While the court ruled that Hansenet/Alice could not "reasonably" be required to block, it based its verdict not on Paragraph 8 of the Telemedia Act, but on the view that the available blocking technology would only have a limited effect. Critics of the ruling argued that it would oblige access providers to block once effective means have been put in place.[25] The types of notification required to trigger the liability of the provider also remained uncertain, as did the extent to which providers could be sued by customers for improperly blocking or removing their content.

Germany is home to a vibrant web community and blogosphere, though the disproportionately young and male population of active users probably affects the mix of topics that are discussed. A great deal of attention is given to telecommunications and internet policies in general, and censorship and surveillance/data-retention issues in particular. A broad public protest against internet censorship in mid-2009 united hackers and digital activists with mainstream bloggers and Twitter users. The protesters launched an e-Petition, which was quickly signed by more than 130,000 people.[26]

[23] "Google-Statistik: Wie die Deutschen Zensur-Vizeweltmeister wurden," *Spiegel Online*, April 21, 2010, http://www.spiegel.de/netzwelt/netzpolitik/0,1518,690278,00.html (in German).
[24] See Google, "Government Requests FAQ," http://www.google.com/governmentrequests/faq.html, accessed September 7, 2010.
[25] Holger Bleich, "Geplante Kinderporno-Sperre könnte andere Sperrverfügungen erleichtern," *Heise Online*, May 14, 2009, http://www.heise.de/newsticker/meldung/Geplante-Kinderporno-Sperre-koennte-andere-Sperrverfuegungen-erleichtern-219091.html (in German).
[26] Markus Beckedahl, "The Dawning of Internet Censorship in Germany," Global Voices Advocacy, June 16, 2009, http://advocacy.globalvoicesonline.org/2009/06/16/the-dawning-of-internet-censorship-in-germany/.

VIOLATIONS OF USER RIGHTS

The German Basic Law safeguards freedom of expression and freedom of the media (Article 5) as well as the privacy of letters, posts, and telecommunications (Article 10). While these articles have also set the standard for the online world, a groundbreaking 2008 ruling by the Federal Constitutional Court declared that the general right of personality guaranteed by Article 2 of the Basic Law "encompasses the fundamental right to the guarantee of the confidentiality and integrity of information technology systems."[27] Unfortunately, these rights have increasingly been contested in a trend that began even before the September 2001 terrorist attacks on the United States.[28] This is particularly worrying with respect to the rights of journalists. Like the clergy, defense lawyers, attorneys, counselors, and various categories of politicians, journalists have been accorded special standing by Paragraph 53 (1) 5 of the code of criminal procedure, which grants them the right to refuse to give evidence. However, the 2001 Act for Limiting the Secrecy of Letters, the Post, and Telecommunications (Article 10 Act–G 10) enables secret services to intercept, monitor, and record private communications, and it differentiates between the protected professions, allowing surveillance of counselors and journalists if the public interest in using their information to combat serious crimes outweighs the public interest in the performance of their professional tasks.

There have been a series of cases in which journalists' rights have been violated. In 2008, it was revealed that the Federal Intelligence Agency (BND) had been following e-mail exchanges between an Afghan politician and an editor at the German weekly *Der Spiegel* for months. The chairman of the Parliamentary Control Panel for the BND at the time voiced his disappointment that the agency had not adopted a stricter attitude toward such matters in the wake of similar scandals in 2006.[29] In fact, a Constitutional Court ruling in February 2007 had set a strong precedent for the protection of journalists' sources.[30] It declared criminal investigations against journalists unconstitutional if the whole or main aim was to

[27] Bundesverfassungsgericht [Federal Constitutional Court], Headnotes to the Judgment of the First Senate of 27 February 2008 on the basis of the oral hearing of 10 October 2007—1BvR 370, 595/07, http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007en.html.

[28] Even the Europe-wide security responses to the 2001 terrorist attacks may be seen as the seamless continuation of an existing trend toward increased surveillance. See David Banisar, *Speaking of Terror: A Survey of the Effects of Counter-terrorism Legislation on Freedom of the Media in Europe* (Strasbourg: Council of Europe, 2008), http://www.coe.int/t/dghl/standardsetting/media/Doc/SpeakingOfTerror_en.pdf.

[29] "German Spies Caught Reading Journalist's E-Mails," Deutsche Welle, April 21, 2008, http://www.dw-world.de/dw/article/0,,3280594,00.html.

[30] Miklós Haraszti, *Access to Information by the Media in the OSCE Region: Trends and Recommendations: Summary of Preliminary Results of the Survey* (Vienna: Organization for Security and Cooperation in Europe, April 30, 2007), 11, http://www.osce.org/documents/rfm/2007/05/24250_en.pdf.

uncover the names of their informants. It further stated that the publication of a functional secret is not sufficient grounds for searching and seizing a journalist's property.[31]

In addition to police authorities and secret services, private companies including the airline Lufthansa and Deutsche Telekom have spied on journalists to identify their sources.[32] In 2008, Deutsche Telekom was found to have abused several hundred thousand sets of telephone traffic data, both landline and mobile, pertaining to journalists, board members, and others, with the goal of tracing information leaks within its ranks.[33] The company had apparently even employed a private detective agency to scan all news on Deutsche Telekom between January 2005 and March 2006 and create a list of journalists to be spied on because they apparently had access to confidential internal information.[34] The company itself acknowledged the "criminal energy" and "methodical malice" apparent in this affair.[35] At the time of writing, the trial had just started, but officials had already been criticized for failing to charge the then chairman of the company's supervisory board and the chief executive, and for delays in the release of crucial information to victims and plaintiffs.[36]

A substantial number of cases involving large companies and their questionable methods of gathering and using data have preoccupied the courts and the public in recent years. For instance, a 2008 case centered on the supermarket chain Lidl, which had comprehensively spied on its employees.[37] In the wake of scandals like these, an amendment to the Federal Data Protection Act was adopted in 2009, adding many provisions to strengthen employees' and users' rights regarding surveillance and unauthorized use of their data.[38] The latest debates on privacy and the practices of internet companies have revolved around Facebook and Google's Street View feature.[39]

While anonymous e-mail services, wireless internet-access points, and public telephone booths have remained legal, mobile-phone users who buy a new contract or

[31] Decision 1 BvR 538/06, 1 BvR 2045/06, February 27, 2007. For the larger European context, see Banisar, *Speaking of Terror*, 15 ff.

[32] "Lufthansa nutzt Passagierdaten für Überwachung," Netzpolitik.org, June 7, 2008, http://www.netzpolitik.org/2008/lufthansa-nutzt-passagierdaten-fuer-ueberwachung/ (in German).

[33] "Telekom bespitzelte Aufsichtsräte, Manager und Journalisten," *Spiegel Online*, May 24, 2008, http://www.spiegel.de/wirtschaft/0,1518,555148,00.html (in German).

[34] "Konzern beauftragte eine Detektei und bespitzelte diverse Reporter," UMTSlink, September 13, 2010, http://www.umtslink.at/3g-forum/news/63161-deutsche-telekom-bespitzelungsaffaere.html (in German).

[35] Deutsche Telekom, "Deutsche Telekom analysiert Tätikeit der früheren Konzernsicherheit," news release, February 10, 2010, http://www.telekom.com/dtag/cms/content/dt/de/812936?printversion=true (in German).

[36] "Telekom-Bespitzelungsaffaire: Journalisten wehren sich gegen Einstellung des Verfahrens," Golem.de, June 28, 2010, http://www.golem.de/1006/76063.html (in German).

[37] See, for instance, Anselm Waldermann, "Spitzel-Skandal: Lidl entschuldigt sich für Stasi-Methoden," *Spiegel Online*, March 26, 2008, http://www.spiegel.de/wirtschaft/0,1518,543597,00.html (in German).

[38] For a summary, see for instance Rhein Main Treuhand, "Datenschutz 2009 Verschärfung und Sanktion," http://www.rhein-main-treuhand.de/aktuelles/200911-datenschutz-2009-verschaerfung-und-sanktion.html (in German), accessed September 13, 2010.

[39] On Facebook, see for instance Maggie Shiels, "Germany Officials Launch Legal Action Against Facebook," British Broadcasting Corporation (BBC), July 8, 2010, http://news.bbc.co.uk/2/hi/8798906.stm. On Google Street View, see Ingo Ruhmann, "Google Street View: Eine politische Kampfansage," *Telepolis*, August 16, 2010, http://www.heise.de/tp/r4/artikel/33/33135/1.html (in German).

prepaid SIM (subscriber identity module) card must register with the network provider. The provider in turn is required to store the user's telephone number, name, address, and birth date; the start date of the contract; and, if applicable, the serial number of the mobile phone for the authorities.[40] Still, a mobile-phone user can achieve anonymity by buying the phone and phone number secondhand, because only the initial user needs to register.[41] Encryption software is freely available and may be used without restrictions.[42]

Law enforcement agencies and prosecutors can obtain users' contractual data without a judge's order under Sections 112 and 113 of the Telecommunications Act. However, judicial approval is required to obtain traffic and content data under Section 113 of the Telecommunications Act and Section 110g of the code of criminal procedure.[43] The Federal Network Agency serves as the data-collection intermediary standing between telecommunications companies and law enforcement bodies, fielding information requests from the latter. The less-protected contractual data is handled automatically, and for the year 2009, the agency reported 4.5 million requests from the authorities and 31.5 million queries directed to telecommunications-service providers.[44] A much smaller number of government entities are authorized, for more narrowly circumscribed purposes, to request more sensitive data under Section 113 of the Telecommunications Act. This data may include personal identity numbers (PINs) and personal unblocking keys (PUKs) that allow access to private terminals or web-based memory-hosting platforms, though the inquiries may only be used to identify the person who generated a certain communication or connection at a certain point in time. The number of requests for these breaches of telecommunications secrecy is reportedly 10 times lower than the number of automated requests for contractual data.[45] However, this would still amount to almost half a million requests in 2009.

Telecommunications interception by state authorities is regulated in Section 100 of the code of criminal procedure, or Strafprozessordnung (StPO). It is understood as a serious interference with basic rights and is subject to proportionality, meaning it may only be employed for the prevention or prosecution of very serious crimes for which specific evidence exists and for which other, less intrusive investigative methods will likely fail.

[40] This is required by Section 111 of the Telecommunications Act and applies to e-mail providers as well. However, it is not specified whether the telecommunications-service providers are required to verify their customers' information.
[41] Torsten Kleinz, "Handy-wechsel-dich," Zeit Online, April 25, 2008, http://www.zeit.de/online/2008/03/handykartenboerse (in German).
[42] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit [Federal Commissioner for Data Protection and Freedom of Information], *Orientierungshilfe zum Einsatz kryptografischer Verfahren* (Berlin: Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, September 2003), http://www.bfdi.bund.de/cae/servlet/contentblob/417366/publicationFile/25259/OrientierungshilfeZumEinsatzKryptografischerVerfahren.pdf;jsessionid=9348094A97AEA15E9D4F6C729361CB6A (in German).
[43] Alexander Schultz, "Auskunftsersuchen der Strafverfolgungsbehörden," Mediendelikte.de, http://www.mediendelikte.de/auskunftsersuchen.htm (in German), accessed September 13, 2010.
[44] The period from 2001 to 2009 shows a steady increase on both counts, from an initial 1.5 million requests from authorities and 3.2 million queries by the Federal Network Agency in 2001. Bundesnetzagentur, *Annual Report 2009*, 125.
[45] Kleinz, "Handy-wechsel-dich."

According to the most recent statistics published by the Federal Office of Justice, in 2008 there were a total of 16,463 orders for telecommunications interception based on Section 100a of the StPO. These referred to fixed-line phones in 3,821 cases, mobile phones in 13,838 cases, and internet communications in 661 cases.[46] Also in 2008, there were a total of 13,904 orders asking for traffic data based on Section 100g of the StPO and Sections 96 (1) and 113a of the Telecommunications Act.[47]

German authorities do not limit themselves to domestic data but also harvest data abroad. In March 2009, *Der Spiegel* reported that the BND had in previous years committed at least 2,500 acts of espionage by remotely searching computers abroad. These searches had at times included the undercover copying of hard drives and transmission of the data to Germany. In other cases they involved the installation of key loggers, which made it possible to track computer keystrokes and thereby gain access to passwords. Among the targets were Pakistani nuclear scientist Abdul Qadir Khan and the Iraqi government's computer system. German agents had also followed the e-mail traffic of an office run by the Welthungerhilfe aid group in Afghanistan. And as noted above, it was revealed in 2008 that the BND had for several months been illegally monitoring e-mail exchanges between Afghan government minister Amin Farhang and a *Spiegel* journalist.[48]

The generalized authority claimed by the BND, whose interceptions are supervised by the parliament's G 10 Commission rather than the judiciary,[49] was seen as particularly excessive at the time because of the landmark February 2008 decision by the Federal Constitutional Court on preventive covert remote computer searches. In its ruling, the court specified that such searches were only permissible "if factual indications exist of a concrete danger" that threatens "the life, limb, and freedom of the individual" or "the basis or continued existence of the state or the basis of human existence." The decision also ruled that any secret infiltration of an information-technology system is "in principle to be placed under the reservation of a judicial order," and that any statute permitting such an infiltration must "contain precautions in order to protect the core area of private life." Even more remarkably, as mentioned above, the court found that the general right of personality

[46] Some orders referred to more than one type of telecommunications interception. Bundesamt für Justiz [Federal Office for Justice], "Übersicht Telekommunikationsüberwachung (Maßnahmen nach §100a StPO) für 2008," July 14, 2009, http://www.bundesjustizamt.de/cln_108/nn_1635504/DE/Themen/Justizstatistik/Telekommunikationsueberwachung/downloads/Uebersicht__TKUE__2008,templateId=raw,property=publicationFile.pdf/Uebersicht_TKUE_2008.pdf (in German).

[47] Bundesamt für Justiz, "Übersicht Verkehrsdatenerhebung (Maßnahmen nach § 100g StPO) für 2008," August 24, 2009, http://www.bundesjustizamt.de/cln_115/nn_1635504/DE/Themen/Justizstatistik/Telekommunikationsueberwachung/downloads/Uebersicht__Verkehrsdaten__2008,templateId=raw,property=publicationFile.pdf/Uebersicht_Verkehrsdaten_2008.pdf (in German).

[48] Holger Stark, "Online-Durchsuchung: BND infiltrierte Tausende Computer im Ausland," *Spiegel Online*, March 7, 2009, http://www.spiegel.de/netzwelt/web/0,1518,611954,00.html (in German).

[49] Daniel Brössler, "Telefonüberwachung: Der Staat hört mit," Sueddeutsche.de, September 22, 2009, http://www.sueddeutsche.de/politik/2.220/telefonueberwachung-der-staat-hoert-mit-1.25048 (in German); Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10), available at http://www.gesetze-im-internet.de/bundesrecht/g10_2001/gesamt.pdf (in German), accessed September 9, 2010.

guaranteed by Article 2 of the German Basic Law "encompasses the fundamental right to the guarantee of the confidentiality and integrity of information-technology systems."[50]

A law that took effect in January 2009 empowered the BKA to conduct covert remote computer searches to prevent terrorist attacks with a judge's permission.[51] Online searches are also an option in very severe criminal cases, with a special responsibility to safeguard the individual's private life and the sensitive data obtained in the search. The law provides immunity from covert remote computer searches to political representatives, the clergy, and defense lawyers, but does not similarly protect doctors and journalists. In addition to computer searches, the act empowers the BKA to employ methods of covert data collection including dragnet investigations, surveillance of private residences, and the installation of a program on a suspect's computer that intercepts communications at their source. So far, the Federal Criminal Court has not availed itself of its new rights.[52] The state government of Rhineland-Palatinate empowered its police force in a similar way, adding the right to interrupt or hinder telecommunications but comprehensively protecting all the professional groups discussed above.

Preventive covert remote computer searches have been defended as a last-resort measure for combating terrorism, but the utility of the tactic has not yet been proven.[53] It has so far been ruled out as a source of evidence for criminal prosecution, and it remains unclear whether it may be used by secret services such as the BND, the Federal and State Offices for the Protection of the Constitution, and the Military Counterintelligence Service (MAD).

Since 1999, the BKA has maintained the Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD), roughly translating as a "central unit for unprovoked searches in data networks."[54] The ZaRD, rather than assisting with existing investigations or pursuing outside tips, actively monitors the internet for signs of unlawful activity in Germany and abroad. Once it has discovered such signs, it can request additional data under Section 113 of the Telecommunications Act, Sections 100g and 100h of the StPO, and Section 7 of the Federal Criminal Office Act, which in turn refers to Section 163 of the

[50] Bundesverfassungsgericht, Headnotes.

[51] Dirk Heckmann, "Anmerkungen zur Novellierung des BKA-Gesetzes: Sicherheit braucht (valide) Informationen," *Internationales Magazin für Sicherheit* nr. 1 (2009), http://www.ims-magazin.de/index.php?p=artikel&id=1255446180,1,gastautor (in German).

[52] Cordula Eubel, "Online-Durchsuchungen – bisher geht es auch ohne," *Der Tagesspiegel*, May 25, 2010, http://www.tagesspiegel.de/politik/online-durchsuchungen-bisher-geht-es-auch-ohne/1844734.html (in German).

[53] It is interesting to note that the same was said about telecommunications interception at the 66th Conference of Federal and State Commissioners for Data Protection, held in Leipzig on September 25–26, 2003. See "Entschließung – Konsequenzen aus der Untersuchung des Max-Planck-Instituts für Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation," http://www.bfdi.bund.de/cae/servlet/contentblob/416440/publicationFile/25103/66DSK-KonsequenzenAusDerUntersuchungDesMax-Planck-InstitutsUeberRechtswirklichkeitUndEffizienzDerUeberwachungDerTelekommunikation.pdf (in German), accessed September 9, 2010.

[54] Its profile can be found at http://www.bka.de/profil/zentralstellen/zard.html (in German), accessed September 9, 2010.

StPO. The ZaRD's investigations uncover 600 to 800 cases of illegal activities annually, of which 70 percent or more involve the storage and dissemination of child pornography.[55]

The BKA reported a total of 50,254 criminal cases in 2009 involving information and communication technologies (ICTs), causing €36.9 million in damages. Almost half of the cases, 22,963, involved computer fraud, and the second-most-common type, at 11,491, centered on illegal data interception and spying.[56] The BKA noted that many more cases are not pursued legally or are not even detected, and that the professional perpetrators, especially international criminal syndicates, constitute a fundamental threat. This argument has been bolstered by the Association for German Criminal Investigators, which sees the internet as the "biggest crime scene of the world."[57] Among other steps, the association calls for mandatory registration with a governmental authority of every user who employs the internet for business transactions, the training of special units to fight computer crimes, and more scope for overt and covert investigations on the internet, especially on social-networking sites.

As of early 2009 there were a total of 80 surveillance facilities maintained by 38 different authorities in Germany. By midyear, a Telecommunications Surveillance Service Center and a Telecommunications Surveillance Competence Center had opened at the Federal Administration Office (Bundesverwaltungsamt) to support the existing surveillance facilities and to start centralizing their activities. The first step in this direction was the linking of the surveillance technologies of the BKA and the Federal Police that year. Critics argued that there was no legal basis for building such "super interception headquarters," and that they would erode the barrier between secret services and police that was incorporated into the constitution as one of the lessons learned from the Nazi era. Moreover, it was unclear how such a centralization of surveillance would safeguard the separation of different investigations and their distinct aims, legal underpinnings, and pools of data.[58]

As noted above, the secret services conduct surveillance under the Act for Limiting the Secrecy of Letters, the Post, and Telecommunications (Article 10 Act–G 10), which enables them to intercept, monitor, and record private communications, and stipulates that their activities are to be governed by the Parliamentary Control Panel, which in turn

[55] An indication of the constancy of this low number of cases and the prevalence of child pornography is provided by Robin O. Debie, "IuK-Kriminalität, mehr als nur Cybercrime: Entwicklung – Stand – Perspektiven," JurPC, 2004, available at http://www.jurpc.de/aufsatz/20040214.html (in German).

[56] Bundeskriminalamt [Federal Criminal Office], *IuK-Kriminalität: Bundeslagebild 2009* (Berlin: Bundeskriminalamt, 2010), 5, http://www.bka.de/lageberichte/iuk/bundeslagebild_iuk_2009.pdf (in German).

[57] Mirko Schubert , „Sicherheit: Kriminalbeamte fordern Notschalter für das Internet," *Netzwelt* (2010), http://www.netzwelt.de/news/83381-sicherheit-kriminalbeamte-fordern-notschalter-internet.html (in German), accessed January 20, 2011.

[58] These points are summarized in two online articles: Klaus C. Koch, "Telekommunikationsüberwachung: Feind hört mit," Sueddeutsche.de, September 14, 2009, http://www.sueddeutsche.de/digital/telekommunikationsueberwachung-feind-hoert-mit-1.28782 (in German); "Superabhörzentral in Köln ohne gesetzliche Grundlage: Datenschützer Peter Schaar kritisiert Bundesverwaltungsamt," Golem.de, August 4, 2009, http://www.golem.de/0908/68812.html (in German).

nominates the members of the G 10 Commission.[59] The latter assesses the necessity of telecommunications surveillance and controls the whole surveillance process. Its chairperson must have the qualifications to serve as a judge. The G 10 Commission is also responsible for overseeing telecommunications measures undertaken on the basis of the Counterterrorism Act of 2002 and the Counterterrorism Amendment Act of 2007. The Parliamentary Control Panel reports periodically to the parliament about the activities of the G 10 Commission and, by extension, of the secret services.[60]

Data retention requirements apply to ISPs and mobile-phone companies, but not to internet cafes. The Federal Constitutional Court struck down a central law on data retention in March 2010, leaving a great deal of uncertainty on this issue.[61] The Law for the New Regulation of Telecommunications Interception and Other Covert Methods of Investigation as well as Compliance with the European Union Directive 2006/24/EG, which took effect in January 2008, had been challenged by more than 30,000 people, including Justice Minister Sabine Leutheusser-Schnarrenberg.[62] It was partly incorporated into the Telecommunications Act, and required telecommunications and internet providers to store all traffic data for six months. The court ruling ordered the deletion of this data. The court argued that the law was unconstitutional because it did not contain any specific measures to keep the data safe and failed to erect enough hurdles for accessing the information. However, the court left open the possibility that a data-retention law could be constitutional, so long as it was limited to facilitating the prosecution of clearly delineated, serious criminal offenses. There would also need to be "transparent control" over what the data could be used for,[63] and the law would have to establish strict procedures to be implemented by telecommunications providers.[64]

Cyberattacks are becoming an important issue in Germany. Citing the private security company G Data, the BKA report for 2009 stated that 350,000 to 700,000 computers—hijacked by hackers and organized into so-called botnets—were put to

[59] See the description on the website of the German parliament, http://www.bundestag.de/htdocs_e/bundestag/committees/bodies/scrutiny/index.html (in German).
[60] See the two briefings by the Parliamentary Control Panel to the parliament in 2010 (Drucksache 17/549 on the measures relating to the Article 10 Act and Drucksache 17/550 on the measures relating to the Counterterrorism Act), both covering the year 2008, available at http://dipbt.bundestag.de/dip21/btd/17/005/1700549.pdf and http://dipbt.bundestag.de/dip21/btd/17/005/1700550.pdf (in German), accessed September 13, 2010.
[61] Bundesverfassungsgericht, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08; verdict available at http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html (in German), accessed September 13, 2010.
[62] Privacy International, "German Federal Constitutional Court Overturns Law on Data Retention," news release, March 9, 2010, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-566038.
[63] It was along these lines that the Federal Constitutional Court limited the use of the law on March 11, 2008, after it received the first formal complaints. Bundesverfassungsgericht, "Eilantrag in Sachen 'Vorratsdatenspeicherung' teilweise erfolgreich," news release, March 19, 2008, http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-037.html (in German).
[64] Bundesverfassungsgericht, "Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß," news release, March 2, 2010, http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011 (in German).

fraudulent use every day in Germany.[65] G Data also enumerated several major cyberattacks for the first half of 2010.[66] For instance, in January, the website of the German Agency for Emissions Trading was subjected to a phishing attack, in the course of which emission allowances were illegally transferred to Denmark and Britain and the perpetrators made up to €3 million. In February, German online news portals such as Golem.de, Handelsblatt.com, and Zeit.de became victims of "malvertising," in which malicious code was downloaded onto the computers of site visitors through infected advertisement banners. In March, the website of the Federal Environment Agency was infected and spread a Zeus Trojan virus for several days. And in May, the data of more than two million students was stolen from the social-networking platform SchülerVZ, apparently in an attempt to alert the site to its security failures.

The German government created the Federal Office for Information Security (BSI) in 1991 to strengthen the security of federal information technology. The act that established the BSI was amended in 2009,[67] giving more leeway to the entity, which has 500 employees. A constitutional complaint has been directed against a paragraph in the amended act that allegedly allows the office to engage in massive data-retention activities.[68]

[65] Bundeskriminalamt, *IuK-Kriminalität: Bundeslagebild 2009*, 10. These numbers should perhaps be viewed with some caution, given that a private provider of security services has an interest in portraying computer crime as a pervasive threat.
[66] G Data issues semiannual malware reports. See Ralf Benzmüller and Sabrina Berkenkopf, *G Data Malware-Report: Halbjahresbericht Januar–Juni 2010* (Bochum: G Data, 2010), http://www.gdata.de/uploads/media/GData_MalwareReport_2010_1_6_DE_mail2.pdf (in German).
[67] Bundesministerium des Innern [Federal Ministry of the Interior], "Act to Strengthen the Security of Federal Information Technology," August 14, 2009, http://www.bmi.bund.de/cln_183/sid_4F946AA4F22A39F6785D8D2AE5F723D9/SharedDocs/Downloads/EN/Gesetzestexte/bsi_act.html?nn=105406.
[68] "Verfassungsbeschwerde gegen BSI-Gesetz eingereicht," Heise Online, September 1, 2010, http://www.heise.de/newsticker/meldung/Verfassungsbeschwerde-gegen-BSI-Gesetz-eingereicht-1070391.html (in German).

INDIA

	2009	2011
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access	12	12
Limits on Content	7	8
Violations of User Rights	15	16
Total	**34**	**36**

POPULATION: 1.2 billion
INTERNET PENETRATION: 5 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Although India's internet penetration rate of less than 10 percent is low by global standards, the country is nonetheless home to tens of millions of users and has become an important leader in the high-tech industry. Meanwhile, access to mobile phones has grown dramatically in recent years, with penetration reaching nearly 60 percent of the population. In the past, instances of the central government and state officials seeking to control communication technologies and censor undesirable content were relatively rare and sporadic. However, since the November 2008 terrorist attacks in Mumbai, which killed 171 people, the need, desire, and ability of the Indian government to monitor, censor, and control the communication sector have grown.[1] Given the range of security threats facing the country, which also include a persistent Maoist insurgency, many Indians feel that the government should be allowed to monitor personal communications such as telephone calls, e-mail messages, and financial transactions.[2] It is in this context that Parliament passed amendments to the Information Technology Act (ITA) in 2008. The changes came into effect in 2009 and have expanded the government's censorship and monitoring capabilities.

The spread of information and communication technologies (ICTs) began accelerating in India with the liberalization of the telecommunications sector as part of the

[1] Joshua Keating, "The List: Look Who's Censoring the Internet Now," *Foreign Policy*, March 24, 2009, http://www.foreignpolicy.com/articles/2009/03/23/the_list_look_whos_censoring_the_internet_now.
[2] "Security Forces, Media, 2 Pillars of Freedom: Poll," *Times of India*, August 15, 2010, http://timesofindia.indiatimes.com/home/sunday-toi/special-report/Security-forces-media-2-pillars-of-freedom-Poll/articleshow/6312697.cms.

New Economic Policy in July 1991.[3] Throughout the early 1990s, various aspects of the telecommunications industry were opened to the private sector, including radio paging and mobile phones.[4] The government's New Telecom Policy of 1999 and New Internet Policy of 1998 have further spurred the growth of the ICT sector,[5] resulting in a large number of manufacturing units and internet-service providers (ISP) setting up bases in the country.

OBSTACLES TO ACCESS

Infrastructure limitations and cost considerations restrict access to the internet and other ICTs in India, though both infrastructure and bandwidth have improved in the last two years. Estimates on internet penetration in India vary considerably. The International Telecommunication Union (ITU) reported 61.3 million users as of 2009,[6] while the Internet and Mobile Association of India (IAMAI) found that about 77 million Indians had used the internet at least once in their lifetimes.[7] A spring 2010 survey by the New Delhi–based research and marketing firm Juxt resulted in an estimate of 51 million "active" internet users, who had used the internet at least once in the past year. (40 million urban and 11 million rural).[8] Despite this confusion, most measurements put the overall internet penetration rate at a rather low 5 to 8 percent of the population. There are signs that this figure is increasing, however, and one recent study predicted that the number of Indian users would reach 237 million in 2015, from a current estimate of 80 million.[9]

Internet use among urbanites appears to be more evenly distributed across the country than several years ago, with the total number of users in towns of under 500,000 people exceeding the total number in the eight largest cities. IAMAI attributes this growth to the prevalence of cybercafes and government e-kiosk initiatives.[10] The latter entail the

[3] Invest India Telecom, "Indian Telecom Sector," Ministry of Communications and Information Technology–Department of Telecommunications, http://www.dot.gov.in/osp/Brochure/Brochure.htm, accessed January 3, 2011.
[4] Ibid.
[5] Telecom Regulatory Authority of India, "New Telecom Policy 1999," http://www.trai.gov.in/TelecomPolicy_ntp99.asp, accessed January 3, 2011; Peter Wolcott, "The Provision of Internet Services in India," in *Information Systems in Developing Countries: Theory and Practice*, ed. R. M. Davison and others (Hong Kong: University of Hong Kong Press, 2005), http://mosaic.unomaha.edu/India_2005.pdf.
[6] International Telecommunication Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#.
[7] Internet and Mobile Association of India (IAMAI), *I-Cube 2009–2010: Internet in India* (Mumbai: IAMAI, 2010), http://www.iamai.in/Upload/Research/icube_new_curve_lowres_39.pdf; IAMAI, *Internet for Rural India: 2009* (Mumbai: IAMAI, 2010), http://www.iamai.in/Upload/Research/Internet_for_Rural_India_44.pdf.
[8] Juxt, *India Online Landscape 2010* (New Delhi: Juxt, 2010), slides, http://www.juxtconsult.com/Reports/Snapshot-of-Juxt-India-Online-Landscape-2010-Press.ppt.
[9] Tripti Lahiri, "India to Have 237 Million Web Surfers in 2015," *India Real Time* (*Wall Street Journal* blog), September 1, 2010, http://blogs.wsj.com/indiarealtime/2010/09/01/india-to-have-237-million-web-surfers-in-2015/.
[10] IAMAI, *I-Cube 2009–2010: Internet in India,* 7. Parsa Venkateshwar Rao Jr., "The 2nd Tech Revolution in Village India," Hardnews, http://www.hardnewsmedia.com/2006/12/686, accessed January 4, 2011.

creation of 100,000 local facilities that would include computers, printers, digital cameras, scanners, projection systems, and telemedicine equipment.

While many of India's users access the internet via cybercafes, the share of urbanite users with home connections has increased to 53 percent, according to one survey.[11] This shift has been driven in part by greater and cheaper access to broadband service. For example, the state-owned ISP Mahanagar Nigam Telephone Limited (MTNL) provides entry-level DSL access at US$1 per month, and US$2 to US$5 per gigabyte for limited-usage plans.[12] Per capita income in India for the 2009–10 fiscal year was estimated at US$930.[13]

There is a pronounced urban-rural divide, with an approximate rural user base of just 6.46 million, and only 4.18 million active users. This represents a tiny fraction of the total rural population of about 800 million,[14] and indicates that there are approximately 10 times more urban internet users than rural internet users in India. While cost is an obstacle, surveys indicate that lack of electricity and especially low computer literacy and awareness of the internet are more significant.[15] Low literacy rates, particularly in English, are also a major impediment. The availability of internet content in India's eight most widely spoken languages is growing, but remains poor. In August 2010, the U.S.-based Internet Corporation for Assigned Names and Numbers (ICANN) approved a proposal by the Department of Information Technology to allow domain names in Hindi, Bengali, Punjabi, Urdu, Tamil, Telugu, and Gujarati.[16] In addition, the U.S.-based software and internet giants Microsoft and Google have launched initiatives to incorporate Indian languages into their programs and services.[17]

Broadband penetration is very limited at 0.74 percent, particularly when compared with an overall teledensity rate of 52.74 percent.[18] According to the Telecom Regulatory Authority of India (TRAI), as of March 2010 there were 8.7 million broadband connections in the country, an increase from 6.2 million a year earlier, and comprising over half of the

[11] Ivinder Gill, "A Wider Net," *Indian Express*, August 13, 2010, http://www.indianexpress.com/news/a-wider-net/659494/0; Juxt, *India Online Landscape 2010*.
[12] Marcos Aguiar and others, *The Internet's New Billion: Digital Consumers in Brazil, Russia, India, China, and Indonesia* (Boston: Boston Consulting Group, September 2010), 17, http://www.bcg.com/documents/file58645.pdf.
[13] "Average Income of Indians to Rise to Rs 43,749 This Fiscal," *Times of India*, February 8, 2010, http://timesofindia.indiatimes.com/business/india-business/Average-income-of-Indians-to-rise-to-Rs-43749-this-fiscal/articleshow/5548821.cms.
[14] Press Information Bureau of India, "Rural Development," http://pib.nic.in/archieve/others/fsrurald.pdf.
[15] IAMAI, "84% of Rural India Not Aware of Internet," news release, September 13, 2010, http://www.iamai.in/PRelease_Detail.aspx?nid=2159&NMonth=9&NYear=2010.
[16] Surabhi Agarwal and Shauvik Ghosh, "Domain Names in Regional Languages Soon," Livemint.com, August 17, 2010, http://www.livemint.com/2010/08/17220818/Domain-names-in-regional-langu.html#.
[17] Ishani Duttagupta and Ravi Teja Sharma, "Google, Microsoft Focus on Regional Languages," *Economic Times*, August 2, 2010, http://economictimes.indiatimes.com/infotech/internet/Google-Microsoft-focus-on-regional-languages/articleshow/6242139.cms.
[18] "TRAI Concerned About Low Broadband Penetration," Cyber Media, June 10, 2010, http://www.ciol.com/News/News/News-Reports/TRAI-concerned-about-low-broadband-penetration/137492/0/.

internet subscriptions in the country.[19] In 2004, the government launched a Broadband Policy with the aim of reaching 20 million broadband subscribers by 2010. Having fallen short of this target, in June 2010 the TRAI initiated a consultation process to develop an improved national broadband policy.[20]

Meanwhile, the government and private companies are working to expand India's conduits to the international internet and build up the broadband infrastructure. The government is planning to roll out a network of 500,000 kilometers of fiber-optic cable to provide villages with high-speed connections, in some cases linking smaller existing networks.[21] India is connected to the international internet through a number of submarine cables, and the private firm Pacnet plans to invest US$150 million to extend a cable to the city of Chennai in the southeast. As a result, after 2012 the supply of international bandwidth available to Indians is expected to vastly increase, which would likely lead to lower end-user prices.[22]

India's overall mobile-phone penetration figures are promising, with almost 60 percent of the population using mobile phones. The TRAI cited the total mobile subscriber base as almost 730 million by December 2010,[23] more than double the 347 million users recorded by the ITU for 2008.[24] Access to the internet through mobile phones has risen as well, apparently due to a series of inexpensive rate plans that service providers introduced in early 2010. Still, only a small percentage of mobile-phone users access the web on their devices. According to IAMAI, an estimated 20 million people had such access in late 2010, up from 12 million in 2009.[25] As of mid-2010, only the state-run Bharat Sanchar Nigam Limited (BSNL) and MTNL offered third-generation (3G) mobile internet services, though several private providers were scheduled to launch 3G services by early 2011.

However, in August 2010 it was reported that the Ministry of Home Affairs (MHA) had asked the Department of Telecommunications to suspend newly introduced 3G mobile service and halt providers' ongoing rollout of the technology, particularly in Jammu and Kashmir. The authorities apparently wanted time to develop the ability to intercept 3G

[19] TRAI, "'Indian Telecom Services Performance Indicator Report' for the Quarter Ending March 2010," news release, July 22, 2010, http://www.trai.gov.in/WriteReadData/trai/upload/PressReleases/744/qpressrelease22jul.pdf.
[20] Nivedita Mookerji, "Stage Set for New Broadband Policy," *Daily News &Analysis*, June 11, 2010, http://www.dnaindia.com/money/report_stage-set-for-new-broadband-policy_1394639.
[21] Thomas K. Thomas, "Special Purpose Vehicle Planned for Broadband Push," *Business Line*, July 23, 2010, http://www.thehindubusinessline.com/2010/07/24/stories/2010072453070100.htm.
[22] Rohin Dharmakumar, "The Long Arm of Broadband," *Forbes India*, February 5, 2010, http://business.in.com/article/breakpoint/the-long-arm-of-broadband/9592/1.
[23] "India's Mobile Phone Users Grow to 729.57 Million," *Economic Times*, January 25, 2011, http://economictimes.indiatimes.com/news/news-by-industry/telecom/indias-mobile-phone-users-grow-to-72957-million/articleshow/7361931.cms.
[24] ITU, "ICT Statistics 2008—Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#.
[25] Archna Shukla, "More People Are Logging On to Internet Via Cellphones," *Indian Express*, August 10, 2010, http://www.indianexpress.com/news/more-people-are-logging-on-to-internet-via-cellphones/658375/0; see also Aguiar, *The Internet's New Billion*.

communications in the volatile region.[26] Short-message service (SMS), or text messaging, has been blocked periodically in Jammu and Kashmir. For example, it was suspended in April 2010 amid popular unrest, but the ban was revoked within days.[27] On September 23, 2010, the Indian government temporarily blocked mass text messages across India in anticipation of a court ruling on a hotly disputed place of worship in Ayodhya. Following the deferment of the verdict date, the ban was extended until September 30.[28]

There are presently no blanket restrictions on accessing advanced web applications like the video-sharing site YouTube, the social-networking site Facebook, or the Twitter microblogging platform. Such sites are becoming increasingly important in India. According to Alexa, Facebook is the third most popular site, followed by YouTube at fifth, the social-networking site Orkut at eighth, and Twitter at tenth.[29]

Three major operators sell international internet bandwidth at the wholesale level: Tata Group's VSNL, Bharti Airtel, and Reliance Globalcom. Since the deregulation of the telecommunications sector in the late 1990s, users in India have been able to choose among hundreds of different public and private service providers. BSNL and MTNL, both state owned, are the two largest ISPs, with a combined 70 percent of subscribers.[30] They retain a dominance established before the appearance of private competitors such as Sify Technologies, Bharti Airtel, and Reliance Communications, each of which controls less than 10 percent of the market.[31] Few of the 104 service providers authorized to offer broadband have been able to penetrate the market given the strong position occupied by BSNL and MTNL.[32] However, both companies have been forced to offer lower rates to stave off the private ISPs.

Private companies have been more successful in the mobile-phone service market. The top 10 providers are Bharti Airtel, BSNL, Vodafone Essar, Reliance Communications, Idea Cellular, Tata Communications, Tata Teleservices, Aircel, MTNL, and Tata Teleservices (Maharashtra) Limited (TTML).[33] Licenses are issued following a bidding process, but launching a mobile-phone service business in practice requires considerable financial clout and access to important government officials. In October 2010, a major corruption scandal involving the licensing of 2G services in 2008 was exposed. Evidence

[26] Mansi Taneja, "Home Ministry Asks DoT to Stop All 3G Services," *Business Standard*, August 10, 2010, http://www.business-standard.com/india/news/home-ministry-asks-dot-to-stop-all-3g-services/404078/.
[27] Agence France-Presse, "Authorities Revoke Text Message Ban in Indian Kashmir," *Taipei Times*, April 18, 2010, http://www.taipeitimes.com/News/world/archives/2010/04/18/2003470823.
[28] "India Bans Bulk Text Messages Before Mosque Verdict," Reuters, September 22, 2010, http://www.reuters.com/article/idUSSGE68M03W20100923.
[29] Alexa, "Top Sites in India," http://www.alexa.com/topsites/countries/IN, accessedFebruary 7, 2011.
[30] TRAI, *The Indian Telecom Services Performance Indicators: January–March 2010* (New Delhi: TRAI, July 2010), http://www.trai.gov.in/WriteReadData/trai/upload/Reports/51/finalperformanceindicatorReport9agust.pdf.
[31] Ibid.
[32] Mookerji, "Stage Set for New Broadband Policy."
[33] "10 Top Telecom Service Providers in India," Rediff.com, August 9, 2010, http://business.rediff.com/slide-show/2010/aug/09/slide-show-1-10-top-telcos-in-india.htm#contentTop.

revealed that the former Telecom Minister, A. Raja, had intentionally favored a few select bidders, including Reliance Communications. By not conducting a competitive auction before granting the licenses, his actions reportedly cost the government up to $39 billion.[34] Raja resigned in November 2010, and was under investigation by a parliamentary public accounts committee at year's end.[35]

Although opening a cybercafe was relatively simple in the past, law enforcement authorities have reportedly complicated the process in recent years. Obtaining a license now requires approval from as many as six different agencies. These difficulties, combined with increases in home and mobile internet connections, have dimmed prospects for new entrants to the cybercafe market.

The TRAI is the main regulatory body for telecommunications matters, with authority over ISPs and mobile-phone service providers. It functions as an independent agency, offering public consultations and other participatory decision-making processes. While it has received some criticism, it is generally perceived as fair. However, the Ministry of Communications and Information Technology (MCIT) and the MHA also exercise control over several aspects of internet regulation, and interventions by the MHA in particular carry considerable weight. There have been no publicized disputes between the ministries and the TRAI to date.[36]

LIMITS ON CONTENT

There has been no sustained government policy or strategy to block access to ICTs on a large scale, though blocks have been imposed sporadically during crises, such as the Kargil war with Pakistan in 1999. Attempts to filter content have mostly originated with state-level executive authorities, and with private individuals through court cases. However, government measures to institute administrative processes for removing certain content from the web, sometimes for fear they could incite violence, have become more common in recent years.

Since 2003, the institutional structure of internet censorship and filtering in India has centered on the Indian Computer Emergency Response Team (CERT-IN), a body created in 2003 within the MCIT's Department of Information Technology. CERT-IN serves as a nodal agency for accepting and reviewing requests from a designated pool of government officials to block access to specific websites. When it decides to block a site, it directs the Department of Telecommunications—also part of the MCIT—to order all licensed Indian

[34] Robert Clark, "India Rocked by 2G Scandal," Telecoms Europe, November 19, 2010, http://www.telecomseurope.net/content/wrap-india-rocked-2g-scandal.
[35] "Indian PM Singh Has 'Nothing to Hide' Over 2G Claims," British Broadcasting Corporation (BBC), December 20, 2010, http://www.bbc.co.uk/news/world-south-asia-12035906.
[36] B. Raman, "The Internal Security Czar," *Outlook*, December 24, 2009, http://www.outlookindia.com/article.aspx?263528.

ISPs to comply with the decision. There is no review or appeals process in place.[37] In June 2009, the authorities blocked a highly popular adult cartoon site called Savitabhabhi without granting the creators an opportunity to defend their right to free expression, raising concerns about the arbitrary nature and broad scope of the government's power in this area.[38] While there is no publicly available list of officially blocked websites, no politically oriented website is believed to have been blocked during the reporting period.

Pressure on private intermediaries to remove certain information in compliance with administrative censorship orders has increased since late 2009, with the implementation of the amended ITA. The revised law grants the MCIT authority to block internet material that is perceived to endanger public order or national security, requires companies to have a designated employee to receive government blocking requests, and assigns up to seven years' imprisonment for representatives of a wide range of private service providers—including ISPs, search engines, and cybercafes—if they fail to comply with government blocking requests. While some observers acknowledge that incendiary online content could pose a real risk of violence, particularly given India's history of periodic communal strife, press freedom and civil liberties advocates have raised concerns over the far-reaching scope of the ITA, its potential chilling effect, and the possibility that the authorities could abuse it to suppress political speech.[39]

When Google began reporting government requests for data and content removal in early 2010, India ranked third in the world for removal requests and fourth for data requests. Between July 1, 2009, and December 31, 2009, India had submitted 142 removal requests, of which 77.5 percent were fully or partially complied with. The requests related to the Blogger blog-hosting service, Book Search, Geo, SMS channels, web searches, YouTube, and especially Orkut.[40] In one case that gained international attention, Google in September 2009 took down an Orkut group on which users had reportedly posted offensive comments about the chief minister of Andhra Pradesh, who had been killed in a helicopter crash a few days earlier. Indian officials were apparently concerned that the comments could spark communal violence.[41]

Google has removed content in response to requests from various government authorities. For example, in January 2007 the company agreed to an arrangement allowing police forces to directly report objectionable content to Google and ask it for details regarding internet protocol (IP) addresses and service providers. By May of that year, Google had cooperated with the Mumbai police regarding online communities and

[37] Keating, "The List: Look Who's Censoring the Internet Now."
[38] K K. Sruthijith, "Govt Bans Popular Toon Porn Site Savitabhabhi.com; Mounting Concerns Over Censorship," contentSutra, June 25, 2009, http://contentsutra.com/article/419-govt-bans-popular-toon-porn-site-savitabhabhi.com-mounting-concern-over/Media/.
[39] Amol Sharma and Jessica E. Vascellaro, "Google and India Test the Limits of Liberty," *Wall Street Journal*, January 4, 2010, http://online.wsj.com/article/SB126239086161213013.html.
[40] Google, "Transparency Report: Government Requests," http://www.google.com/governmentrequests/.
[41] Sharma and Vascellaro, "Google and India Test the Limits of Liberty."

comments directed against the Indian historical figure Shivaji, right-wing leader Bal Thackeray, and dalit leader B. R. Ambedkar.[42]

Bloggers are rarely forced by the government or private individuals to take down their writings, but there have been a few instances in which this has occurred.[43] For example, blogger Chetan Kunte criticized NDTV journalist Barkha Dutt for her station's coverage of the November 2008 terrorist attack on Mumbai, accusing her of engaging in sensationalism and irresponsibly airing information about the movements of security forces. Dutt and NDTV threatened to seek punitive measures against Kunte through the courts, and the blogger agreed to remove the critical content.

While online journalists and bloggers are not often required to censor their writing, it is understood that certain topics must be approached with caution. These include religion, communalism, the corporate-government nexus, links between government and organized crime, Kashmiri separatism, hostile rhetoric from Pakistan, and various forms of aggressive, demagogic speech. Such topics are indeed addressed by online writers, but they are handled carefully to avoid inciting violence, particularly by nonstate actors.

Highly partisan reporting and commentary abound on the Indian internet, stemming from real or perceived divisions between the government and the people, between ethnic and religious communities, and between India and some of its regional neighbors. Such material is especially common on left- or right-wing extremist sites and sites related to Kashmir.

The Indian blogosphere is quite active and eloquent, complementing the rise in internet use by different interest groups and civil society actors. However, the actual number of bloggers still appears to be quite small, and the blogosphere is fragmented given the large number of blogging platforms available.

Online communication and social-networking services are increasingly being used as means to organize politically. Various politicians, including the 87-year-old former deputy prime minister L. K. Advani,[44] use social media and ICTs to reach out to voters. In the run-up to the 2009 general elections, political parties and their allies mounted massive SMS campaigns to drum up support.[45] Citizens also mounted online campaigns on various issues, including one protesting the phenomenon of accused or convicted criminals running for

[42] "Objectionable Postings on Shivaji, Thackeray: Cops Trace IP Addresses," Expressindia.com, May 4, 2007, http://cities.expressindia.com/fullstory.php?newsid=234691; "Google, Police to Clean Up Orkut," *Times of India*, May 5, 2007, http://timesofindia.indiatimes.com/Google_police_to_clean_up_Orkut/articleshow/2005902.cms.

[43] Paul Bradshaw, "TV Station Forces Blogger to Withdraw Criticism of Its Coverage," *Online Journalism Blog*, February 2, 2009, http://onlinejournalismblog.com/2009/02/02/tv-station-sues-blogger-for-criticising-its-coverage/.

[44] Advani's blog can be found at http://blog.lkadvani.in/.

[45] "BJP Gets Help from Unofficial 'SMS Campaign,'" *Financial Express*, February 24, 2009, http://www.financialexpress.com/news/bjp-gets-help-from-unofficial-sms-campaign/427422/; Joji Thomas Philip and Harsimran Singh, "Cellphone Users Bombarded With Political Info," *Economic Times*, March 10, 2009, http://economictimes.indiatimes.com/News/News-By-Industry/Telecom/Cellphone-users-bombarded-with-political-info/articleshow/4247903.cms.

seats in Parliament. Other sites aimed to educate voters about candidates' backgrounds,[46] or aggregate election-related news articles.[47] A collaborative online platform called Vote Report India allowed citizens to share information on violations of electoral rules using media including SMS, e-mail, and Twitter.[48]

VIOLATIONS OF USER RIGHTS

The Indian constitution, particularly Article 19, protects freedom of speech and expression.[49] Along with the right to life and liberty under Article 21, Article 19(1)(a) has also been held to apply to the privacy of telephone conversations, and established guidelines regulate the ability of state officials to intercept communications.[50]

ICT usage is governed primarily by the Telegraph Act, the penal code, the code of criminal procedure, and the ITA. The 2008 amendments to the ITA, which took effect in October 2009,[51] raised concerns about an expansion of state surveillance capacity, including interception of SMS and e-mail messages. Several provisions of the revised law entail possible restrictions on users' rights.

For example, the changes considerably broadened the scope of activities identified as criminal offenses under the act, which now include sending messages that are deemed offensive, dishonestly receiving stolen computer resources or communication devices, identity theft, impersonation, violation of bodily privacy, cyberterrorism, and the publication or transmission of sexually explicit material. The prescribed punishments vary, but many offenses carry up to three years in prison. Under the revised Section 80, lower-ranking police officers are permitted to conduct personal searches and arrests without a warrant in public spaces and private businesses that are accessible to the public, provided there is a reasonable suspicion that a crime covered under the act has been or is about to be committed.

Section 69 expands the circumstances under which communications may be monitored, intercepted, and decrypted. Previously, such surveillance was governed by the 1885 Telegraph Act, which allowed it only during times of "public emergency" or in the "interests of the sovereignty and integrity of India." The amended ITA drops these and other

[46] See Jaago Re at http://jaagore.com/.
[47] One such site was Blogadda at http://indianelections.blogadda.com/.
[48] See Vote Report India at http://votereport.in/.
[49] http://lawmin.nic.in/coi/coiason29july08.pdf.
[50] *PUCL v. Union of India* (1997) 1 SCC 301. See also Vikram Raghavan, *Communications Law in India* (London: LexisNexis Butterworths, 2007), 760–761.
[51] The amended act is available at http://www.naavi.org/ita_2008/ch1_2008.htm.

limitations. Section 69B, for instance, allows the central government to collect traffic data from any computer source without a warrant, whether the data are in transit or in storage.[52]

Critics of the ITA amendments have also raised concerns that the law does not adequately protect personal information held by private corporations. Although the changes require corporations handling sensitive personal data to maintain "reasonable security practices and procedures," the rules are not clearly defined, and it remains unclear how they will be enforced.[53]

Internet users have sporadically faced prosecution for online postings, and private companies hosting the content are obliged by law to hand over user information to the authorities. In September 2007, after Google and a major ISP cooperated with a police investigation, information-technology worker Lakshmana Kailash K was jailed for 50 days for allegedly defaming an Indian historical figure online. It later emerged that another person had posted the material, and Kailash was arrested based on the wrong IP address.[54] In May 2008, two men were arrested and charged for posting derogatory comments about Congress party chief Sonia Gandhi on Orkut; the case is still pending.[55] As in the 2007 case, Google, which owns Orkut, accommodated the authorities' request for identity information.[56] In July 2010, a magazine editor in the southern city of Kerala was arrested on defamation charges for an article posted on the magazine's website about an Indian businessman residing in Abu Dhabi.[57]

In 2009, the Supreme Court ruled that both bloggers and moderators can face libel suits and even criminal prosecution for comments posted by other users on their websites. The case stemmed from several anonymous comments criticizing the right-wing party Shiv Sena that appeared on a web community moderated by a 19-year-old from Kerala, Ajith D. The party's youth wing filed a criminal complaint against Ajith, who asked the Supreme Court to quash the case before it proceeded further, but the court rejected his request.[58]

The overall level of ICT surveillance in India remains unclear, though a series of scandals and new measures in recent years have raised concerns over wide powers granted to security agencies to monitor communications. Intercepts of telephone conversations are allowed under guidelines prescribed by the Supreme Court, and are admissible as evidence.

[52] "Yes, Snooping's Allowed," *Indian Express*, February 6, 2009, http://www.indi.anexpress.com/news/yes-snoopings-allowed/419978/0.
[53] Pavan Duggal, "We're Not Keeping Pace," Cyberlaws.net, http://www.cyberlaws.net/itamendments/TOI1.html, accessed January 8, 2011.
[54] Ketan Tanna, "Wrong Man in Jail for 50 Days on Cyber Charge," *Times of India*, November 3, 2007, http://timesofindia.indiatimes.com/india/Wrong-man-in-jail-for-50-days-on-cyber-charge/articleshow/2513737.cms.
[55] Gloria D Souza, "Man Jailed for Posting Obscene Content on Orkut," Merinews, May 19, 2008, http://www.merinews.com/article/man-jailed-for-posting-obscene-content-on-orkut/134255.shtml.
[56] John Kennedy, "India: Google Assists Police in Orkut User's Arrest," Global Voices Advocacy, May 22, 2008, http://advocacy.globalvoicesonline.org/2008/05/22/india-google-assists-police-in-orkut-users-arrest/.
[57] International Federation of Journalists (IFJ), "Editor's Arrest Underlines Need for Defamation Law Reform," International Freedom of Expression eXchange, July 5, 2010, http://www.ifex.org/india/2010/07/06/nandakumar_arrested/.
[58] Shreya Roy Chowdhury, "Bloggers Unite Against SC Verdict," *Times of India*, February 25, 2009, http://timesofindia.indiatimes.com/India/Bloggers-unite-against-SC-verdict/articleshow/4185938.cms#ixzz10pXLwgS6.

For example, the MHA intercepted mobile-phone communications between the gunmen and their Pakistan-based handlers during the Mumbai terrorist attacks in 2008. These communications were then used as evidence in court.[59] With respect to internet communications, anecdotal accounts indicate that the government's Intelligence Bureau began using a keyword-based interception system in addition to targeted IP-address interception as far back as 2001.

In May 2010, the news magazine *Outlook* published transcripts of phone tapping that recorded individuals including lawmakers from the ruling party.[60] The calls, made on mobile phones at a range of different times and locations were reportedly intercepted and recorded using a new GSM monitoring device. By the end of the year, another major scandal had erupted over the leaking of hundreds of intercepted 2009 phone conversations between lobbyist Niira Radia and an assortment of politicians, bureaucrats, and journalists.[61] The records revealed evidence of corruption and other abuses, and triggered a lawsuit against the government by Radia's employer, business tycoon Ratan Tata, who argued that his privacy rights had been breached. The government responded with the claim that Radia was being monitored as a suspected agent of foreign intelligence services.[62] Lastly, in the context of a corruption investigation related to a former telecommunications minister, the mobile-phone provider Reliance Communications reported to the Supreme Court that the authorities had submitted over 150,000 phone tapping requests from early 2006 to the end of 2010, an average of 30,000 requests per year.[63] The public uproar surrounding these scandals prompted proposals for a law specifying private companies' obligations with respect to wiretap requests from the authorities. The government was also reportedly planning a commission to adjudicate complaints related to such surveillance.[64]

Prior judicial approval for communications interception is not required under either the Telegraph Act or the ITA, and the revised ITA grants both central and state governments the power to issue directives on interception, monitoring, and decryption. All licensed ISPs are obliged by law to sign an agreement that allows Indian government authorities to access user data, though the providers may lack the technical capacity to respond to some requests. For example, in September 2010, ISPs claimed that they would be unable to comply with a

[59] *Mumbai Attack Terror Tape—Phone Conversation Part1* (YouTube, February 26, 2009), 10 min., 34 sec., http://www.youtube.com/watch?v=1PSauTty9LA.
[60] Saikat Datta, "We, the Eavesdropped," *Outlook*, May 3, 2010, http://www.outlookindia.com/article.aspx?265191.
[61] "800 New Radia Tapes," *Outlook*, December 10, 2010, http://www.outlookindia.com/article.aspx?268618.
[62] "2G Scam: Spy Link Sparked Niira Radia Phone Tap," *Hindustan Times*, December 10, 2010, http://www.hindustantimes.com/2G-scam-Spy-link-sparked-Niira-Radia-phone-tap/Article1-636886.aspx#; "'Foreign Agent' Plaint Led to Radia Phone Tap: Govt," South Asian Media Net, December 11, 2010, http://mediawitty.com/test/NewsDetail.aspx?group_id=0&id=10622&folder_id=12&Page_Title=%E2%80%98Foreign%20agent%E2%80%99%20plaint%20led%20to%20Radia%20phone%20tap:%20Govt.
[63] Dhananjay Mahapatra, "Over 1 Lakh Phones are Tapped Every Year," *Times of India,* February 15, 2011, http://timesofindia.indiatimes.com/india/Over-1-lakh-phones-are-tapped-every-year/articleshow/7498154.cms.
[64] "Government Mulling Law to Regulate Phone Tapping," *Daily News & Analysis*, December 16, 2010, http://www.dnaindia.com/india/report_government-mulling-law-to-regulate-phone-tapping_1481790.

Department of Telecommunications notice requiring them to enable the interception of BlackBerry messages for national security reasons (see below).[65]

The national government is reportedly in the process of centralizing its telecommunications monitoring apparatus, which is currently divided among a variety of security agencies and ministries. The overhaul would speed up the collection and processing of intercepted information, integrate disparate databases, and eliminate the need for manual intervention by private companies.[66]

Although the situation may vary from state to state, user anonymity is restricted in many cybercafes, as the operators are required to record certain basic user details in registries. The record of each visitor has to be kept for six months, with details including name, address, identification card information, reason for use of the cafe, and contact numbers. Some cybercafes voluntarily exceed these requirements by requesting a passport photo for their records, demanding explanations if users are visiting a cybercafe outside their own localities, or retaining user files for as long as three years.

Moreover, cybercafes are often subjected to intimidation by local police. There have been anecdotal reports of police instructing owners to retain information like Permanent Account Numbers (PANs)—tax-related numbers that the largely youthful clientele would probably lack. Pressure for more rigorous collection of user data has reportedly increased since September 2010, when an anonymous e-mail message took credit for a recent terrorist attack on Taiwanese tourists in New Delhi.[67] With respect to mobile phones, the Department of Telecommunications has instructed operators to issue and activate mobile SIM cards only after users register their personal details with the carrier.

India has emerged as a leader among countries urging telecommunications companies to reveal their codes or provide other ways for the authorities to intercept their traffic. Indian officials have cited the 2008 Mumbai gunmen's use of mobile and satellite phones to plan and execute their attacks. Also of concern to New Delhi are Chinese companies' growing stake in the telecommunications infrastructure market, which raises fears of infiltration or sabotage, given the two countries' historic rivalry and previous Chinese cyberespionage efforts.[68] Under guidelines issued in July 2010, equipment suppliers are required to allow the local operator, the government, or designated third-party agencies to

[65] Manoj Gairola, "Cannot Meet BlackBerry Deadline, Say Telecom Firms," *Hindustan Times*, September 21, 2010, http://www.hindustantimes.com/Cannot-meet-BlackBerry-deadline-say-telecom-firms/H1-Article1-603125.aspx#.

[66] Joji Thomas Philip, "India Begins Testing CMS to Track All Communications," *Economic Times*, August 18, 2010, http://economictimes.indiatimes.com/news/news-by-industry/telecom/India-begins-testing-CMS-to-track-all-communications/articleshow/6332906.cms.

[67] Rahul Tripathi, "Latest IM Mail To Be Used as Evidence in Batla Case," *Times of India*, September 27, 2010, http://timesofindia.indiatimes.com/city/delhi/Latest-IM-mail-to-be-used-as-evidence-in-Batla-case/articleshow/6633326.cms.

[68] See John Markoff and David Barboza, "Researchers Trace Data Theft to Intruders in China," *New York Times*, April 5, 2010, http://www.nytimes.com/2010/04/06/science/06cyber.html?_r=1. The report by the Information Warfare Monitor and the Shadowserver Foundation, *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, is available at http://www.infowar-monitor.net/2010/04/shadows-in-the-cloud-an-investigation-into-cyber-espionage-2-0/.

"inspect the hardware, software, design, development, manufacturing facility and supply chain, and subject all software to a security threat check."[69] The new rules have met with significant objections from international companies, who warn that they exceed previous international practice.[70] The Swedish firm Ericsson is among those that have resisted the rules,[71] while the Chinese company ZTE was the first to accept them.[72]

The government threatened to shut down BlackBerry services altogether in 2010, demanding that the device's manufacturer, Research in Motion (RIM), provide it with the capacity to read encrypted e-mail and instant messages sent via BlackBerry.[73] The dispute remained unresolved at year's end, after Indian authorities rejected RIM's proposed solutions to the decryption problem.[74] In September 2010, India's home secretary warned that RIM, Google, and Skype could be required to operate their services from locally based servers, enabling closer monitoring by security agencies.[75] Meanwhile, as noted above, the government has threatened to block the introduction and expansion of 3G mobile service across the country until operators provide sufficient means for security-related interception. The companies were still negotiating with the authorities at year's end.[76]

There have been no reports of government agents physically attacking bloggers or online activists. However, given India's complex ethnic, religious, and linguistic make-up, verbal intimidation and concerns over the threat that online postings might spark communal violence, attacks from Maoists, or reprisals from religious extremists lead many online writers to be cautious about what they post.

After scandals emerged of individuals from China infiltrating the Indian military and National Security Council,[77] there are some indications that India is preparing an offensive cyberwarfare capability. According to press reports in August 2010, the government was

[69] Devidutta Tripathy, "Govt Tightens Telecom Rules on Security Concerns," Reuters, July 28, 2010, http://in.reuters.com/article/idINIndia-50466220100728.
[70] Erika Kinetz, "Tough Indian Telecom Rules Spark Foreign Backlash," *R&D Magazine*, August 3, 2010, http://www.rdmag.com/News/FeedsAP/2010/08/information-tech-tough-indian-telecom-rules-spark-foreign-backlash/ .
[71] John Ribeiro, "Ericsson Objects to New Indian Telecom Rules," *Network World*, August 6, 2010, http://www.networkworld.com/news/2010/080610-ericsson-objects-to-new-indian.html.
[72] Surajeet Das Gupta, "ZTE Agrees to Abide by New Telecom Security Rules," *Business Standard*, August 9, 2010, http://www.business-standard.com/india/news/zte-agrees-to-abide-by-new-telecom-security-rules/403960/.
[73] Bappa Majumdar, "BlackBerry Assures India on Access to Services," Reuters, August 13, 2010, http://www.reuters.com/article/idUSTRE67151F20100813; Mark Lee, "RIM Says BlackBerry Should Be Treated Equally as India Threatens Shut Down," Bloomberg, August 13, 2010, http://www.bloomberg.com/news/2010-08-13/rim-says-blackberry-should-be-treated-equally-as-india-threatens-shut-down.html.
[74] Kalyan Parbat and Joji Thomas Philip, "DoT Rejects BlackBerry's Email Decoding Solution," *Economic Times*, October 1, 2010, http://economictimes.indiatimes.com/news/news-by-industry/telecom/DoT-rejects-BlackBerrys-email-decoding-solution/articleshow/6661267.cms.
[75] Bibhudatta Pradhan and Ketaki Gokhale, "India Asks RIM, Google, Skype to Build Local Servers," Bloomberg, September 2, 2010, http://www.businessweek.com/news/2010-09-02/india-asks-rim-google-skype-to-build-local-servers.html.
[76] "Telecom Firms Ask Government Not to Stop 3G Phone Services," Big News Network, December 21, 2010, http://feeds.bignewsnetwork.com/?sid=722420.
[77] Information Warfare Monitor and Shadowserver Foundation, "Shadows in the Cloud: Investigating Cyber Espionage 2.0," April 6, 2010, http://www.nartv.org/mirror/shadows-in-the-cloud.pdf.

considering a plan to enlist civilian professionals in efforts to hack the computer systems of hostile powers.[78]

[78] Harsimran Singh and Joji Thomas Philip, "Spy Game: India Readies Cyber Army to Hack Into Hostile Nations' Computer Systems," *Economic Times*, August 6, 2010, http://economictimes.indiatimes.com/news/news-by-industry/et-cetera/Spy-Game-India-readies-cyber-army-to-hack-into-hostile-nations-computer-systems/articleshow/6258977.cms.

INDONESIA

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Partly Free**
Obstacles to Access	n/a	14
Limits on Content	n/a	13
Violations of User Rights	n/a	19
Total	**n/a**	**46**

POPULATION: 235.5 million
INTERNET PENETRATION: 18 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Digital communication in Indonesia has developed rapidly since 1994, when the first commercial internet-service provider (ISP) introduced it to the public. This growth has expanded avenues for freedom of expression and access to information for ordinary Indonesians. In particular, the popularity of social-networking applications has grown exponentially, with Indonesia becoming home to some of the largest contingents of Twitter and Facebook users in the world.

However, the authorities have also sought to regulate online content in recent years. In the process, a number of actions taken, including passage of the Law on Information and Electronic Transactions (ITE Law) of 2008, have fallen short of international democratic standards. In 2009 and 2010, there were several incidents in which platforms for user-generated content were blocked, at least eight individuals have faced prosecution for comments made online, and the government has considered implementing regulations that would require ISPs to filter certain content, including information of political consequence. Together, these measures and an atmosphere of legal uncertainty have raised concerns that in the near future greater restrictions on internet freedom could emerge. Bloggers, civil society groups, and ISPs have resisted such efforts via online mobilization and advocacy, in some instances successfully fending off new restrictions or reversing existing ones.

OBSTACLES TO ACCESS

Access to the internet has grown dramatically since 1998, when the government reported that only 0.26 percent of the population had used the medium.[1] By 2009, Indonesia had an estimated 20 million internet users, according to the International Telecommunications Union (ITU).[2] In June 2010, the Ministry of Communications and Information Technology (MCI) reported that the number had reached 45 million, or approximately 18 percent of the population.[3] Access has not been evenly distributed across the country due to poverty and poor infrastructure in rural areas. Given Indonesia's archipelagic geography, cable infrastructure has been costly to provide and is mostly confined to urban areas, particularly on the islands of Java and Bali. Consequently, although the number of broadband internet connections has doubled since 2006,[4] broadband service remains prohibitively expensive or otherwise unavailable to many Indonesians. A personal broadband internet connection currently costs 75,000 to 160,000 Indonesian rupiah (US$8-14) per month; by comparison, the average monthly per capita income among the poorest segments of the population is 200,000 rupiah (US$22),[5] and in Jakarta the minimum wage for workers is about 1.1 million rupiah (around US$122) per month.[6] Most of those with home broadband connections are therefore middle- or upper-class urban residents, particularly in cities on Java. Cybercafes have played a key role in enabling internet access to penetrate every corner of Indonesia at a relatively low price.

The growth of internet access via mobile phones has been a positive development, as prices are relatively affordable and the cost of the necessary infrastructure is far less than for cable broadband. Telkomsel, the largest mobile-phone service provider, has reported that mobile-phone internet service is available in all major cities and the capitals of all regencies.[7]

---

[1] International Telecommunication Union, "ICT Statistics 2000—Internet," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2000&RP_intLanguageID=1&RP_bitLiveData=False.

[2] International Telecommunication Union, "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

[3] Ardhi Suryadhi, "Pengguna Internet Indonesia Capai 45 Juta"[Indonesian Internet Users Reach 45 Million], Detikinet, June 9, 2010, http://us.detikinet.com/read/2010/06/09/121652/1374756/398/pengguna-internet-indonesia-capai-45-juta.

[4] BuddeComm, *2007 Asia—Telecoms, Mobile and Broadband in Indonesia and Timor Leste* (Bucketty, Australia: BuddeComm, 2007), http://www.budde.com.au/Research/2007-Asia-Telecoms-Mobile-and-Broadband-in-Indonesia-and-Timor-Leste.html.

[5] Badan Pusat Statistik, Jumlah dan Presentase Penduduk Miskin, Garis Kemiskinan, Indeks Kedalaman Kemiskinan, dan Indeks Keparahan Kemiskinan, Menurut Propinsi, pada Maret 2009, [Central Bureau of Statistics, Number and Percentage of Poor Population, Poverty Line, Poverty depth index, and index of severity of Poverty, by Province, March 2009], http://www.bps.go.id/tab_sub/view.php?tabel=1&daftar=1&id_subyek=23&notab=3.

[6] "UMP Jakarta 2010 Naik 4,5 Persen" [Jakarta Per Capita Minimum Wage increases 4.5 percent in 2010], Kompas.com, November 13, 2009, http://megapolitan.kompas.com/read/2009/11/13/18491935/UMP.Jakarta.2010.Naik.4.5.Persen.

[7] Chanuka Wattegama, Juni Soehardjo, and Nilusha Kapugama, "Telecom Regulatory and Policy Environment in Indonesia: Results and Analysis of the 2008 TRE Survey," March 18, 2008, p. 8 [henceforth "TRE Survey"], http://www.lirneasia.net/wp-content/uploads/2009/07/TRE_Indonesia_2009Mar18.pdf.

Such widespread service, together with the proliferation of cheaper phones and related devices, has contributed to a drastic increase in the number of internet users over the past two years. Between June 2008 and June 2009, the number of mobile internet users rose from 300,000 to over one million.[8]

The Indonesian government, and especially the MCI, has made the expansion of internet usage a priority. It has decreased tariffs on fixed-line and mobile-phone use, and launched a program to establish so-called Smart Villages (Desa Pintar), which would have good internet access and mobile-phone reception. The aim is to enable all villages to have internet access by 2014.[9] Separately, civil society groups have promoted the RT/RW Net product, despite the fact that it is currently prohibited by the government. The system uses wireless technology to allow multiple users to share a broadband connection, thereby reducing the cost of access per household significantly.[10]

The video-sharing site YouTube, the social-networking site Facebook, and international blog-hosting services are generally available without interference. Indeed, the number of Indonesian Facebook users has grown exponentially in recent years, from 2 million in 2009 to over 30 million by the end of 2010, the second most users in the world.[11] However, in April 2008 the minister of communication and information sought to limit circulation of the anti-Islamic Dutch film *Fitna* in Indonesia after coming under pressure from groups such as the Majelis Ulama Indonesia (MUI), the country's official council of Muslim clerics. The minister ordered ISPs to "immediately use all effort to block all sites and blogs which post the *Fitna* movie." ISPs across the country consequently blocked access to content-sharing sites including YouTube, MySpace, Multiply, RapidShare, and Metacafe. In response, several corporations filed lawsuits against the Association of Indonesian Internet Service Providers (APJII), requesting compensation for lost marketing and advertising revenue, while individual users circulated petitions urging the government to retract the ban on the applications. After about a week, the government yielded to public pressure and withdrew its order.[12]

[8] Spire Research and Consulting, "Indonesia: Asia's Mobile Internet Success Story," *Spire E-Journal* (December 2009), http://www.spireresearch.com/pdf/archive/ejournal-dec09/Indonesia-%20Asia%27s%20mobile%20internet%20success%20story.pdf.

[9] Suci Astuti, "Depkominfo Sampaikan Program Kerja 100 Hari" [The Ministry of Communication and Information Conducts a 100 Day Program], Elshinta Radio, November 23, 2009, http://www.elshinta.com/v2003a/readnews.htm?id=82635.

[10] Harry Sufehmi, "Kalengbolic, Solusi Internet Kecepatan Tinggi & Murah Meriah" [Kalengbolic, The Fastest and Cheapest Internet Solution], *Harry.Sufehmi.com* (blog), April 7, 2008, http://harry.sufehmi.com/archives/2008-04-07-1628/; interview with Harry Sufehmi, Second Deputy Chairperson of Open Source Association of Indonesia (AOSI) and information-technology practitioner, May 17, 2010.

[11] Nick Burcher, "Facebook Usage Statistics—March 2010 (with 12 month increase figures)," *Nick Burcher* (blog), March 31, 2010, http://www.nickburcher.com/2010/03/facebook-usage-statistics-march-2010.html.

[12] Geoff Thompson, "Indonesia Bans YouTube, MySpace," Australian Broadcasting Corporation (ABC), April 10, 2008, http://www.abc.net.au/news/stories/2008/04/10/2212779.htm?section=entertainment; "Download Surat 'Ultimatum' Menkominfo Untuk Pemblokiran" [Download the Warning Letter from The Ministry of Communication and Information on (internet) Blocking], Detikinet, April 4, 2008, http://www.detikinet.com/index.php/detik.read/tahun/2008/bulan/04/tgl/04/time/175015/idnews/918570/idkanal/447

The government responded more mildly in May 2010 when an account on Facebook promoted a competition to draw the prophet Muhammad. Organizations including the Islamic Group Forum and the Indonesian Student Action Muslim Union urged the government to ban Facebook,[13] but rather than issuing instructions to block the full application, the authorities sought to focus their censorship measures on the account in question. Officials sent a letter to Facebook urging closure of the account, asked all ISPs to limit access to the account's link as the content was in violation of the ITE Law, and invited the Indonesian Association of Internet Cafe Entrepreneurs to restrict access to the group. Due to opposition from bloggers and civil society, however, ISPs disregarded the government's requests, and the account remained accessible. While commending the decision not to fully block Facebook, free expression advocates raised concerns over government officials' attempt to use the incident to energize plans to censor the internet more systematically.[14]

Indonesia has a range of privately-owned digital media service providers, though some are known to have close ties to government ministers. As of 2007, there were 298 ISPs operating throughout Indonesia, the six largest being Bakrie Telecom, Indosat, Indosat Mega Media, Telkom, Telkomsel, and dan XL Axiata.[15] This dominance, together with regulatory obstacles imposed by the government, have created a significant barrier for small ISPs to enter the market legally. As of early 2010, there were 9 mobile-phone service providers, of which the most prominent were PT Telkomsel, PT Indosat, and PT XL Axiata, with Telkomsel itself covering 50 percent of the market.[16] The country's main network-access providers (NAPs), which link retail-level ISPs to the internet backbone, are concentrated on Java, and particularly in Jakarta.

Government permission is required to develop internet infrastructure and establish cybercafes, and some analysts have attributed the lack of infrastructure in much of the country to ineffective regulation and restrictive government policies.[17] The MCI, with its Directorate General of Post and Telecommunication (DGPT), is the primary body

[13] Hanin Mazaya, "Panggil ISP, Menkominfo akan blokir Facebook?" [Call your ISP, The Minister of Communication and Information will block Facebook?], Arrahmah.com, May 20, 2010, http://www.arrahmah.com/index.php/news/read/7894/panggil-isp-kominfo-akan-blokir-facebook.

[14] Aliansi Jurnalis Independen [Alliance of Independent Journalists] (AJI), "RPM Konten Multimedia adalah 'sensor 2.0'" [Multimedia content of RPM is Censor 2.0], news release, May 20, 2010, http://www.ajiindonesia.org/index.php?option=com_content&view=article&id=224:aji-rpm-konten-multimedia-adalah-sensor-20&catid=14:alert-bahasa-indonesia&Itemid=287.

[15] Ministry of Communication Information Technology (MCI), "Press Conference of Minister of Kominfo Tifatul Sembiring on Preparation of Plan for Blocking Internet Porn," press release, August 10, 2010, http://bit.ly/9N8NWk.

[16] Hendarsyah Tarmizi, "Mergers and acquisitions inevitable in mobile phone industry," *Jakarta Post,* March 1, 2010, http://www.thejakartapost.com/news/2010/03/01/mergers-and-acquisitions-inevitable-mobile-phone-industry.html; Direktorat Jenderal Pos dan Telekomunikasi, Kementerian Komunikasi dan Informasi, Buku Statistik Bidang Pos dan Telekomunikasi 2009, [The Directorate General of Post and Telecommunication, The Ministry of Communication and Information, Statistics Book on Post and Telecommunication 2009], http://www.postel.go.id/webupdate/Download/Data_Statistik_Smt-1_09.pdf; TRE Survey, 9.

[17] TRE Survey, 12.

overseeing telephone and internet services; it is responsible for issuing licenses for ISPs, cybercafes, and mobile-phone service providers. In addition, the Indonesia Telecommunication Regulation Body (BRTI) conducts regulation, supervision, and control functions related to telecommunications services and networking. In practice, there is an unclear overlap between the mandates and work of the two agencies. Based on the ministerial decree that established it, BRTI is supposed to be generally independent and includes nongovernment representatives. However, observers have questioned its effectiveness and independence, as it is headed by the DGPT director, and draws its budget from DGPT allocations.[18]

LIMITS ON CONTENT

The introduction of the internet has expanded Indonesians' access to information, as they are no longer dependent on traditional media (television, radio, and newspapers) for news. Many Indonesians, especially those from the urban middle and upper classes, have adopted the internet as their main information source. In response, the government's approach to the internet has shifted as well. In March 2008, the government passed the ITE Law, which broadened the authority of the MCI to include supervision of the flow of information and possible censorship of online content.[19] Since then, several initiatives have raised the possibility of increased censorship, though none appear aimed at systematically targeting content critical of the government or current administration. Strong opposition from civil society and, to an extent, from ISPs has successfully derailed some such plans.

Following enactment of the ITE Law, the ministry began exploring ways to restrict content deemed to constitute a disturbance to public order, but few measures had been taken by the end of 2009. In early 2010, the ministry published a draft Regulation on Multimedia Content that, if implemented, would require ISPs to filter or otherwise remove certain material. The types of content listed include vaguely worded categories such as pornography, gambling, hate incitement, threats of violence, exposure of private information, intellectual property, false information, and content that degrades a person or group on the basis of a physical or nonphysical attribute, such as a disability.[20] The regulation

[18] TRE Survey, 16.

[19] Article 40(2) of ITE Law states that "the government, in compliance with the prevailing laws and regulations, aims at protecting public interest from all forms of disturbances that result from the abuse of electronic information and electronic transaction. Law No. 11 of 2008 on Electronic Transaction and Information, available at http://www.setneg.go.id/components/com_perundangan/docviewer.php?id=1969&filename=UU%2011%20Tahun%202008.pdf.

[20] Ministry of Communication and Information, "Tentang Sikap Kementerian Kominfo Dalam Menyikapi Peningkatan Maraknya Penyalah-Gunaan Layanan Internet" [About the Ministry of Communication and Information's Stance in Addressing the Increase of Internet Service Abuse], news release, February 11, 2010, http://www.depkominfo.go.id/berita/siaran-pers-no-22pihkominfo22010-tentang-sikap-kementerian-kominfo-dalam-menyikapi-peningkatan-maraknya-penyalah-gunaan-layanan-internet/ .

also calls for the creation of a Multimedia Content Screening Team, which many fear would essentially function as an internet censorship body.[21] The team would consist of 30 people and be headed by the DGPT director; half of the members would be government officials, and the other half would come from civil society, most likely from groups closely affiliated with the government.[22] The panel's tasks would include identifying websites with illegal content, and taking punitive measures, such as imposing fines or revoking the licenses of providers that enable the content's continued circulation. The draft regulation includes no procedure for appeals of a team decision; while affected users might file a civil suit, that would not be a practical or timely remedy for inappropriate content removal, given the Indonesian courts' already large backlog of cases.

The announcement of the draft regulation prompted strong opposition from society, especially from ISPs and journalists.[23] The Alliance of Independent Journalists (AJI) raised concerns over the vague wording and broad range of information that would be affected, as well as the creation of a government-run content control institution, particularly one that would target advanced web applications. It argued that such a mechanism would not be in compliance with the Indonesian constitution or the Press Law, and urged the government to instead set up a more diverse, multi-stakeholder commission to regulate internet content.[24] Following the public outcry, the government announced that it would take time to process suggestions from the public before proceeding with the draft regulation.[25] Nevertheless, the proposal was not formally terminated, prompting fears that it might be resurrected in the future.

To date, the authorities are not known to have placed any restrictions on content addressing political issues, criticizing the authorities, or spreading ideology that is not in line with that of the government. However, in August 2009, after arresting Muhammad Jibril, publisher of a radical Islamist website and magazine,[26] for allegedly arranging funding for bombings at two hotels in Jakarta the previous month, the authorities temporarily shut

[21] Enda Nasution, "Selamat Datang Lembaga Sensor Internet Indonesia" [Welcome to the Institute of Indonesian Internet Censorship], Politikana, February 12, 2010, http://www.politikana.com/baca/2010/02/12/selamat-datang-lembaga-sensor-internet-indonesia.html.

[22] Carolina Rumuat, "SOS Internet Indonesia," Global Voices, February 17, 2010, http://globalvoicesonline.org/2010/02/17/sos-internet-indonesia/.

[23] Southeast Asian Press Alliance, "Media Group Asks Indonesian Minister to Junk Controversial Internet Regulation Draft," news release, March 18, 2010, http://www.seapabkk.org/newdesign/alertsdetail.php?No=1235.

[24] Aliansi Jurnalis Independen [Alliance of Independent Journalists] (AJI), "RPM Konten Multimedia adalah 'sensor 2.0'" [Multimedia content of RPM is Censor 2.0], news release, May 20, 2010, http://www.ajiindonesia.org/index.php?option=com_content&view=article&id=224:aji-rpm-konten-multimedia-adalah-sensor-20&catid=14:alert-bahasa-indonesia&Itemid=287.

[25] Bagus BT Saragih, "Tifatul to Ease Back from Pushing Through Web Bill," *Jakarta Post*, February 25, 2010, http://www.thejakartapost.com/news/2010/02/25/tifatul-ease-back-pushing-through-web-bill.html.

[26] "Situs Ar-rahmah Milik Muhammad Jibril Tak Bisa Diakses" [Arrahmah website of Muhammad Jibril is not accessible], Metro TV News, August 26, 2009, http://metrotvnews.com/index.php/metromain/newsvideo/2009/08/26/89056/Situs-Ar-rahmah-Milik-Muhammad-Jibril-Tak-Bisa-Diakses.

down his website, Arrahmah.com.[27] In addition, in July 2010, the DGPT issued a letter ordering all ISPs to block access to websites carrying pornography. The instructions left the decision of which particular websites to filter in the hands of the ISPs themselves.[28] Although the letter is not fully legally binding, by December 2010, six of the largest ISPs had reportedly complied with the request. Many smaller ISPs provided subscribers with the option to choose for such content to be blocked. In practice, users wishing to nonetheless access the websites have had little trouble circumventing the censorship.

Some restrictions on content have been carried out under pressure from private actors, sometimes with ties to prominent politicians, as occurred with the Okezone online news website, a subsidiary of the MNC media group, one of Indonesia's largest.[29] In 2008, the Attorney General's Office uncovered a corruption scandal involving the Directorate General of General Legal Administration in the Law and Human Rights Ministry. Among those implicated in the scandal was a top executive of the MNC group. The company's owners subsequently intervened in and directed Okezone's coverage of the scandal. Okezone's reporters were required to dedicate a disproportionate share of their reporting to one of the accused in the scandal, Sarana Rekatama Dinamika, or to Yusril Ihza Mahendra, then minister of law and human rights. An AJI report analyzing the coverage found that of 80 reports on the scandal, Okezone cited Dinamika as its primary source 16 times, and Mahendra 15 times. Only 10 citations referred to the attorney general's office.[30] Okezone also deleted from its website information considered unfavorable to Dinamika. Queries to Okezone's internal search engine turned up 81 news titles that mentioned the scandal, but only 48 of the articles were actually accessible.[31]

The development of Indonesia's blogosphere began between 1999 and 2000, with most early blogs written by Indonesians living abroad and working in the field of information technology. In 2001, the younger generation came to dominate Indonesian blogs, largely writing about their daily lives. By 2005 and 2006, blogs had begun to specialize in various topics, including politics, economics, media, food, and entertainment. The number of bloggers reached 50,000 by the end of 2006, and according to blogger Enda Nasution, the figure ballooned to 1.2 million by 2009.[32] Only a few blogs play a watchdog

[27] Agence France-Presse, "Indonesia Arrests Second Man Over Bomb Funds: Police," *Hindustan Times*, August 26, 2009, http://www.hindustantimes.com/Indonesia-arrests-second-man-over-bomb-funds-police/Article1-447051.aspx.

[28] Reporters Without Borders, "Government Orders ISPs to start Anti-Porn Filtering," International Freedom of Expression eXchange (IFEX), August 11, 2010, http://www.ifex.org/indonesia/2010/08/11/anti_porn_filtering/.

[29] According to a survey by Alexa Internet in April 2009, Okezone was ranked as the 23rd most visited website in Indonesia. Okezone uploaded on average 300 news articles a day. MNC group is one of the biggest media groups in Indonesia. It owns television stations such as RCTI, TPI, Global TV, and SUN TV, and newspapers such as *Seputar Indonesia* and *Kanal Okezone*. Further information is available at http://www.mnc.co.id/.

[30] "Geger di Sisminbakum, Sunyi di RCTI dan Okezone, dalam Wajah Retak Media: Kumpulan Laporan Penelusuran," [Dispute in Sisminbakum, Quiet at RCTI and Okezone, the Negative Face of Media: Fact Finding Report] (Jakarta: AJI Indonesia, 2009).

[31] Ibid.

[32] Stefanus Yugo Hindarto, "Blogger Belum 'Jamah' Indonesia Timur" [Bloggers not yet reached Eastern Indonesia], Okezone, June 21, 2010, http://techno.okezone.com/read/2010/06/21/55/345116/.

role by scrutinizing government activities, although these blogs have been extremely important in exposing incidents of corruption. They are typically maintained by nongovernmental organization (NGO) activists, human rights lawyers, or journalists.

The internet as a whole nevertheless serves as an important source of information on political issues and related discussions. In the run-up to the 2009 presidential election, the use of Google searches to seek out information about candidates grew exponentially, with searches for incumbent president Susilo Bambang Yudhoyono increasing by 625 percent, and those for his main challenger, Megawati Sukarnoputri, rising by 40 percent between January and July.[33] Similarly, research noted an increase in Facebook postings citing the term "jilbab," which in Indonesia refers to a Muslim woman's headscarf; the topic had become a wedge issue during the campaign.[34]

Civil society groups have used the internet to mobilize and advocate against government censorship plans. After the enactment of the ITE Law, NGOs formed a coalition called the Indonesia National Alliance on Cyber Law Reform (ANRHTI). It consisted of the Indonesian Legal Aid and Human Rights Association (PBHI), the Institute for Criminal Justice Reform (ICJR), the Institute for Policy Reform and Advocacy (ELSAM), the Indonesian Legal Aid Foundation (YLBHI), the AJI, and the Legal Aid Center for Press (LBH Pers).

One prominent example of effective mobilization against internet censorship was the case of housewife Prita Mulyasari, one of the first people brought to court under the ITE Law. She was arrested in May 2009, held for three weeks, and charged with defamation for an e-mail message she circulated to friends and relatives in which she criticized her treatment at a private hospital in Tangerang. The PBHI published a press release on Prita's detention,[35] and she soon gained popular support, including from bloggers; five NGOs submitted an amicus brief to the Tangerang District Court in October, as it was examining her criminal defamation case.[36] In December, the Banten High Court ruled against Prita in her appeal of the parallel civil case, ordering her to pay 204 million rupiah (US$19,600) in damages to the Omni International Hospital.[37] The blogging community responded with a huge campaign called Koin Keadilan, or Justice Penny, and succeeded in collecting more

[33] Scott Hartley, "Google: Tomorrow's Silicon (Not Crystal) Ball," *Internet and Democracy Blog*, July 15, 2009, http://blogs.law.harvard.edu/idblog/2009/07/15/electionprediction/.
[34] Scott E. Hartley, "Reading Google in Jakarta," *Foreign Policy*, July 6, 2009, http://www.foreignpolicy.com/articles/2009/07/06/reading_google_in_jakarta?page=0,1.
[35] Nadya Kharima, "UU ITE Makan Korban Lagi" [ITE Bill creates a victim again], Primaironline, May 28, 2009, http://primaironline.com/berita/detail.php?catid=Sipil&artid=uu-ite-makan-korban-lagi.
[36] "Kasus Prita: Lima LSM Ajukan 'Amicus Curiae'" [Prita case: 5 NGOs submit Amicus Curiae], Kompas.com, October 14, 2009, http://megapolitan.kompas.com/read/2009/10/14/16474375/Kasus.Prita:.Lima.LSM.Ajukan..quot.Amicus.Curiae.quot.
[37] Cyprianus Anto Saptowalyono, "Humas PT Banten: Putusan buat Prita belum berkekuatan hukum tetap" Banten Corporate Public Relations: Verdict for Prita does not have legal power], Kompas.com, December 7, 2009, http://m.kompas.com/news/read/data/2009.12.07.13135791.

than 600 million rupiah on her behalf.[38] By the end of 2009, the hospital had decided to drop the civil suit, and Prita won her criminal case in Tangerang District Court, which acquitted her on all charges.[39] Nevertheless, her case and other prosecutions under the ITE Law have contributed to an increased atmosphere of caution and self-censorship among online writers and average users. The public campaign against the proposed Regulation on Multimedia Content also utilized online platforms, with many Indonesians submitting their protests directly to the communication and information minister's Twitter account, or writing about the issue on their blogs.[40]

Another incident reflecting the growing role of social media in political mobilization in Indonesia stemmed from charges filed against the leadership of the Indonesian Anti-Corruption Commission (KPK). In November 2009, the national police declared the two KPK deputy chairs, Bibit Samad Riyanto and Chandra Hamzah, to be extortion suspects. After wiretap recordings revealed a conspiracy to discredit the widely respected KPK, and many came to believe that the new arrests were part of the plot, an ordinary Indonesian citizen set up a Facebook group called "Gerakan 1.000.000 Facebookers dukung Chandra Hamzah & Bibit Samad Riyanto," (The Movement of 1 million Facebookers to support Chandra Hamzah & Babit Samad Riyanto),[41] which quickly grew to more than half a million members, and had 1.3 million by August 2010.[42] As of December 2010, the attorney general's office reportedly planned to drop the charges, under a legal provision enabling such action to protect the "public interest."[43]

VIOLATIONS OF USER RIGHTS

The constitution guarantees freedom of opinion in its third amendment, adopted in 2000.[44] The guarantee also includes the right to privacy and the right to gain information and

[38] Mega Putra Ratya, "Penghitungan selesai total koin Prita Rp. 650.364.058" [Counting of Coins for Prita has collected a total of Rp. 650,364,058], Detikcom, December 19, 2009, http://m.detik.com/read/2009/12/19/113615/1262652/10/penghitungan-selesai-total-koin-prita-rp-650364058.

[39] Ismira Lutfia, Heru Andriyanto, Putri Prameshwari, and Ronna Nirmala, "Prita Acquitted, But Indonesia's AGO Plans Appeal," *Jakarta Globe*, December 29, 2009, http://www.thejakartaglobe.com/home/prita-mulyasari-cleared-of-all-charges/349844; Yudi Rahmat, "PBHI Apresiasi putusan hakim PN Tangerang di Kasus Prita" [PBHI appreciates verdict of Tangerang State Court judge in Prita Case], Primaironline, December 29, 2009, http://primaironline.com/berita/detail.php?catid=Sipil&artid=pbhi-apresiasi-putusan-hakim-pn-tangerang-di-kasus-prita.

[40] For example, prominent blogger Antyo Rentjoko's writings about the draft regulation can be found at http://blogombal.org/2010/02/13/mendidik-masyarakat-siapa-mendidik-siapa.

[41] The Facebook group is located at http://facebook.com/group.php?gid=169178211590.

[42] Peter Gelling, "Indonesia: Corruption Junction," GlobalPost, November 9, 2009, http://www.globalpost.com/dispatch/indonesia/091106/indonesia-corruption-kpk.

[43] "Police Admit They Have No Recordings in Bibit and Chandra Case," *Jakarta Globe,* August 11, 2010, http://www.thejakartaglobe.com/home/police-admit-they-have-no-recordings-in-bibit-and-chandra-case/390619; Peter Gelling, "Indonesia: Corruption Junction," GlobalPost, November 9, 2009, http://www.globalpost.com/dispatch/indonesia/091106/indonesia-corruption-kpk.

[44] Constitution of 1945, Article 28E(3).

communicate freely.[45] These rights are further protected by various laws and regulations.[46] However, a range of other laws are used to limit free expression, despite legal experts' claims that they conflict with the constitution.[47] Approximately seven different laws address internet freedom in one aspect or another; this legal framework is fairly harsh, although the authorities do not always use the full range of powers granted by the laws.

In addition to the controversies mentioned above involving potential internet censorship under the 2008 ITE Law, other provisions of the law have raised concerns, as they have been used to prosecute users for online expression. In particular, the ITE Law has enabled heavier penalties for criminal defamation than those set out in the penal code. Anyone convicted of committing defamation online may face up to six years in prison, and a fine of up to 1 billion rupiah (US$111,000).[48] As of June 2010, there were at least eight cases in which citizens had been indicted on defamation charges under the ITE Law for comments on e-mail lists, blogs, or Facebook.[49] In some of the cases, the accused users were temporarily detained at the beginning of the process. One of these was the high-profile case of housewife Prita Mulyasari, described above. In another case from February 2010, teenager Nur Farah, from Bogor in West Java, was convicted based on a report that she had insulted one of her friends by addressing her as a "dog" on Facebook.[50] Journalist and blogger Nurliswandi Piliang was charged under the ITE Law in 2008. He and three other bloggers—Edy Cahyono, Nenda Inasha Fadillah, and Amrie Hakim—filed a petition to the Constitutional Court with the help of ANRHTI, but the court upheld the law in May 2009.[51] While there have been some discussions among government agencies about amending the ITE Law, no concrete action had been taken as of December 2010.

In terms of indecency on the internet, Law No. 44 of 2008 on Pornography defines the crime of "pornography" very broadly, and includes requirements for supervision of users at cybercafes. The government is reportedly planning to enhance implementation of such

[45] Ibid., Articles 28F and 28G(1).

[46] Among others, Law No. 39 of 1999 on Human Rights, available at http://www.legalitas.org/incl-php/buka.php?d=1900+99&f=uu39-1999eng.htm ; Law No. 14 of 2008 on Freedom on Information, available at http://www.setneg.go.id/components/com_perundangan/docviewer.php?id=1971&filename=UU%2014%20Tahun%202008.pdf ; and Law No. 40 of 1999 on the Press, available at http://www.legalitas.org/incl-php/buka.php?d=1900+99&f=uu40-1999.htm.

[47] Wahyudi et al., "Elsam, Asesmen Terhadap Kebijakan Hak Asasi Manusia dalam Produk Legislasi dan Pelaksanaan Fungsi Pengawasan DPR RI" [Assesment to the Human Rights Policy in Legislation Product and the Implementation of the Parliament Monitoring Function], 2008. Hard copy on file with the author.

[48] ITE Law, Article 45.

[49] Supriyadi W. Eddyono, "Tabulasi Kasus Pidana Penghinaan dengan Menggunakan UU ITE" [Tabulation of Criminal Defamation Cases using the ITE Law], Institute for Media Defense Litigation Network (IMDLN), 2009. Hard copy on file with the author.

[50] Anwar Hidayat, "Terbukti Menghina Lewat Facebook, Farah Divonis 2 Bulan Bui" [Proven to have insulted someone through Facebook, Farah sentenced to 2 months in Jail], Detik.com, February 16, 2010, http://www.detiknews.com/read/2010/02/16/134623/1300580/10/terbukti-menghina-lewat-facebook-farah-divonis-2-bulan-bui.

[51] Perhimpunan Bantuan Hukum dan HAM Indonesia (Indonesian Association for Legal Aid and Human Rights), "Pasal 27 ayat (3) UU ITE tidak bisa ditafsirkan secara sewenang [Article 27 paragraph (3) of the ITE cannot be arbitrarily interpreted], press release, May 5, 2009 https://anggara.files.wordpress.com/2009/05/siaran-pers-pengujian-pasal-27-ayat-3-uu-ite.pdf.

supervision by pushing through the Draft Law on Computer Crimes. The draft stipulates numerous restrictions on computer and internet usage, often prescribing harsher penalties for offenses already covered in the criminal code and other legislation. Passage of the new measure would bring to eight the number of laws regulating criminal defamation, with each calling for a different sentence; however, the law was pending at year's end.

Also under discussion has been a draft law on ICT convergence, one that would collectively replace the Telecommunications Law, Broadcasting Law, and possibly the ITE Law. Critics have raised concerns that under the law, ICT applications (including websites) would be required to obtain a license from the MCI for a fee, a process that could place restrictions on freedom of expression, as well as for the open source community[52] and expansion of WiFi hotspots. [53]

Abusive surveillance practices are not a serious concern in Indonesia, although there is little oversight or checks in place to prevent abuse by agencies conducting monitoring for the purposes of combating terrorism and identifying terrorist networks, the most known use of surveillance techniques. At present, only the State Intelligence Body (Badan Intelijen Negara, or BIN),[54] the police,[55] the KPK,[56] and the National Narcotics Board (Badan Narkotika Nasional) have the legal authority to conduct surveillance.[57]

Indonesia has at least nine laws that allow the authorities to conduct surveillance or wiretapping.[58] The only one that explicitly states the need for judicial oversight is Law No. 35 of 2009 on Narcotics, and even in that instance the requisite procedures are unclear. Forthcoming regulations called for in the ITE Law may provide a more unified and coherent procedure for conducting surveillance, but the article is currently being challenged by human rights activists before the Constitutional Court.

---

[52] Taken from his tweet @sufehmi on 8 October 2010, 23:30, Harry Sufehmi is 2nd Deputy Chairperson of AOSI and IT Practitioner.

[53] Interview with Harry Sufehmi, 2nd Deputy Chairperson of AOSI and IT Practitioner.

[54] Presidential Decision No. 103 of 2001, available at http://www.setneg.go.id/components/com_perundangan/docviewer.php?id=1476&filename=Keputusan_Presiden_no_103_th_2001.pdf; Minister of Communication and Information Regulation No. 01/P/M.KOMINFO/03/2008 on the Recording of Information for the Purposes of the State's Defense and Security, available at http://anggara.files.wordpress.com/2009/12/permen-kominfo-perekaman-informasi.pdf.

[55] Law No. 16 of 2003 on the Stipulation of Government Regulation in Lieu of Law No. 1 of 2002 on the Eradication of Crimes of Terrorism (State Gazette No. 46 of 2003, Supplement to the State Gazette No. 4285), available at http://www.setneg.go.id/components/com_perundangan/docviewer.php?id=1548&filename=PP_Pengganti_UU_No_1_th_2002.pdf.

[56] Law No. 30 of 2002 on the Anti-Corruption Commission, available at http://www.setneg.go.id/components/com_perundangan/docviewer.php?id=300&filename=UU_no_30_th_2002.pdf.

[57] Law No. 35 of 2009 on Narcotics, available at http://www.setneg.go.id/components/com_perundangan/docviewer.php?id=2351&filename=UU%2035%20Tahun%202009.pdf.

[58] The laws are, among others, (1) Chapter XXVII Indonesian Criminal Code, Article 430—434; (2) Law No. 5 of 1997 on Psychotropic Drugs; (3) Law No. 31 of 1999 on Eradication of Corruption; (4) Law No. 36 of 1999 on Telecommunication; (5) Government Regulation in Lieu of Law No. 1 of 2002 on Combating Terrorism; (6) Law No. 18 of 2003 on Advocates; (7) Law No. 21 of 2007 on Combating Human Trafficking; (8) Law No. 11 of 2008 on Electronic Transaction and Information; and (9) Law No. 35 of 2009 on Narcotics.

In terms of anonymity, mobile-phone users are obliged to register their numbers upon purchasing a phone by submitting their identity information directly to the government via text message. In practice, however, this obligation is often ignored. The government has taken steps to pressure the Canadian company Research in Motion (RIM) to set up local servers and filter pornography for its Blackberry devices in Indonesia, considering the growing number of such users, and concerns that the encrypted communication network would hinder anti-terrorism and anti-corruption efforts.[59]

There have been no reports of extralegal attacks, intimidation, or torture of bloggers or other internet users. However, it is common for police to conduct searches of cybercafes without prior notice to the owners, since these venues are generally perceived as places conducive to accessing pornography; some searches are carried out by nonstate actors such as Islamic fundamentalist groups as well. According to various reports, these searches are conducted fairly regularly in different parts of the country, particularly in cities with a large student population, partly with the aim of catching those skipping school to get online.[60] Most of the searches are conducted without warrants and are rarely followed up with court proceedings. Moreover, the raids are also seen as a means for police to extract bribes from cybercafe owners.

[59] "Indonesia Says Blackberry Will Filter Out Porn," Associated Press, January 11, 2011, http://ipolitics.ca/2011/01/11/indonesia-says-blackberry-to-filter-out-porn/; John Ribeiro, "Indonesia Presses RIM Over its Blackberry Service," Network World, August 5, 2010, http://www.networkworld.com/news/2010/080510-indonesia-presses-rim-over-its.html.

[60] "Police Bust High School Students for Cutting Class in Favor of Facebook," *Jakarta Globe,* March 3, 2010, http://www.thejakartaglobe.com/home/police-bust-high-school-students-for-cutting-class-in-favor-of-facebook/361673; "Indonesia rounds up students in cybercafés," *Agence France-Presse,* February 23, 2010, http://newsinfo.inquirer.net/breakingnews/infotech/view/20100223-254794/Indonesia-rounds-up-students-in-cybercafs.

IRAN

	2009	2011
INTERNET FREEDOM STATUS	Not Free	Not Free
Obstacles to Access	21	21
Limits on Content	24	29
Violations of User Rights	31	39
Total	76	89

POPULATION: 75.1 million
INTERNET PENETRATION 2009: 24.5 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Since the protests that followed the disputed presidential election of June 12, 2009, the Iranian authorities have waged an active campaign against internet freedom, employing extensive and sophisticated methods of control that go well beyond simple content filtering. These include tampering with internet access, mobile-telephone service, and satellite broadcasting; hacking opposition and other critical websites; monitoring dissenters online and using the information obtained to intimidate and arrest them; ordering blogging service providers inside Iran to remove "offensive" posts or blogs; and trying to fill the information vacuum created by these measures with propaganda and misinformation.

The Iranian regime has long had an ambivalent relationship with the internet, viewing it alternately as a catalyst for economic development and diversification or as an invading force that threatens the state's strict social, religious, and political values. The internet was first introduced by the government in the 1990s to support technological and scientific progress in an economy that had been deeply affected by eight years of war with Iraq. However, until 2000, the state played an insignificant role in the growth of internet use among the Iranian public. In this period the private sector was the main driver of internet development, leaving the state with the challenging task of keeping up with a dynamic and overwhelmingly youthful society. The government of the reformist president Mohammad Khatami (1997–2005) then invested heavily in expanding the internet infrastructure, but during his administration, the authorities began to clamp down on free expression in both the traditional media and online.

Supreme Leader Ali Khamenei first asserted control over the internet through a May 2001 decree and subsequent legislation by the Cultural Revolution High Council that forced all internet service providers (ISPs) to end their direct connections, obtain a license to operate, and purchase their bandwidth from government-controlled Access Service Providers.[1] The regime's ferocious attacks on internet use after the 2009 election seemed to mark the end of its internal debate, as the leadership decisively chose political control over the benefits of a more open society.

OBSTACLES TO ACCESS

The Khatami administration, following an economic development plan devised during the last term of President Akbar Hashemi Rafsanjani, worked to connect different cities with fiber-optic cables and increase the Iranian internet's connection points to the global network. The result of this and other such efforts was an explosion in internet use in the country. According to the International Telecommunication Union (ITU), there were 625,000 internet users in Iran at the beginning of 2000. By the end of Khatami's presidency in 2005, the number had increased to several million. This period also featured a major demographic shift in Iran. The population had increased tremendously since the end of the Iran-Iraq war, to a point where more than 70 percent of the population was born after the 1979 revolution. Faced with restrictions on most other forms of expression and social interaction, this young population turned to the internet in large numbers. At the same time, the cost of internet access remains very high and the service is mostly available in the cities, meaning users are predominantly urban middle and upper class. A report prepared by Iran's parliament blames the government for holding a monopoly on internet bandwidth and selling it to users through a number of intermediaries.[2] Direct access to the internet via satellite is only permitted to certain institutes, and it remains prohibited for personal use.

Statistics relating to the number of internet users in Iran are inconsistent and highly disputed, even among Iranian officials. The single official source of data is the ITU, which receives statistics from the government on different information and communications technology (ICT) indicators. According to official sources, the Iranian government calculates the number of internet users by forecasting the number of potential users based on the available bandwidth. Therefore, the reported numbers do not correspond to the actual number of Internet users at all. According to a survey conducted in 2009 by Iran Statistics Centre and published in March 2010, the internet penetration rate in Iran stood at 11 percent; 30 percent of the internet users were based in Tehran; and the penetration rate was

[1] "Country Profile—Iran," OpenNet Initiative, June 16, 2009, http://opennet.net/research/profiles/iran.
[2] Iran ICT News, "Identifying the causes behind the expensiveness of the Internet in Iran," October 10, 2010, http://tinyurl.com/33vpzjf.

15 percent in urban and 3 percent in rural areas. This is significantly lower than the internet penetration reported to the ITU the same year, which was approximately 38 percent.

The internet and its users played an important role in the opposition movement following the June 2009 presidential election, in which incumbent Mahmoud Ahmadinejad was accused of winning a new term through fraud. After the authorities barred international media from directly covering the opposition protests and ensuing violence by security forces, foreign outlets came to rely on user-generated content posted on the internet from inside Iran. The regime characterized these interactions between protesters, internet users, and international media as a "soft war" orchestrated by foreign powers, and vowed to combat it in kind. The government has reportedly allocated $500 million in its 2010–11 annual budget for this purpose.

During the protests, authorities curbed internet access by introducing 60 to 70 percent packet loss into the network, resulting in a massive drop in speed.[3] This came in the context of an existing 128-kilobyte bandwidth limitation imposed on private broadband users beginning in 2006.[4] By March 2009, there were only around 557,857 broadband subscribers in Iran, the majority of private users are connected with 56kb to the internet.[5] Given these obstacles, it became difficult to conduct basic online activities like opening e-mail messages or viewing simple webpages.[6] The government blamed the slowdown on damage to undersea cables in the Persian Gulf, but the timing was very much aligned with key protests, which strongly suggests that the authorities were in full control of internet speed. Similarly, during protest days many of the important network ports used by instant-messaging and chat platforms were also tampered with, resulting in partial or complete loss of function for these tools.

As of December 2010, all the major international social-networking and media-sharing websites like Facebook, YouTube, and Flickr were blocked, while some file types, such as MP3 audio files, have been sporadically filtered. The periodic filtering and disruption of services based overseas—such as Google's fairly well-encrypted e-mail and blogging platforms, Gmail and blogger.com—appear designed to frustrate users and eventually force them to seek more easily monitored alternatives based in Iran. Although many Iranians have been able to access the blocked platforms and content by using various circumvention techniques, the authorities have actively worked to disrupt such efforts, forcing users to constantly adapt and search for new solutions.

According to official statistics, there are approximately 54 million mobile-phone subscriptions in Iran. Mobile-telephone service was also subject to government controls.

[3] Packet loss occurs when one or more packets of data traveling across a computer network fail to reach their destination.

[4] "Iranian Government: Internet Speed is Good" (in Persian), BBC, May 21, 2010 http://www.bbc.co.uk/persian/iran/2010/05/100521_l38_iran_internet_speed_taghipour.shtml.

[5] The association of private broadband service providers in Iran, "official stats on available broadband ports in Iran until March 19, 2010 " http://www.adsl-pap.com/fa/port/.

[6] It takes 6 minutes to download a MP3 music file with 128kb connection and 12 minutes with 56kb connection.

Mobile-phone text messaging, or short-message service (SMS), was shut down throughout Iran the day before the election and did not resume until 40 days later. Subsequently it was disrupted on a temporary basis immediately before and during key protests days. There have been reports that messages with banned keywords were filtered even when service was up. However, any use of SMS by dissenters in Iran is very limited and highly risky. Users must present some form of identification when purchasing mobile-phone subscriptions, making it an easy task for the authorities to track down the authors and recipients of specific messages.

The period after the election featured a broad assertion of power by the Islamic Revolutionary Guards Corps (IRGC), a politically important branch of the security forces that also controls large sections of the economy. Even as it managed the government's crackdown in the streets, it used its economic muscle to increase state dominance of the information landscape. In September 2009, for example, the IRGC purchased a controlling stake in the Telecommunication Company of Iran (TCI), the country's main provider of internet and mobile-telephone service. The second mobile operator, IranCell, is owned in part by a web of proxy companies controlled by the IRGC (there are a number of high profile IRGC ex-commanders among its management). The third operator, due to be launched in early 2011, is a government-owned entity.

LIMITS ON CONTENT

Internet filtering, which began toward the end of the Khatami presidency in 2005, has become more severe since the June 2009 election. The authorities now employ a centralized filtering system that can effectively block a website within a few hours across the entire network in Iran. Private internet-service providers (ISPs) were forced to either use the bandwidth provided by the government or route their send traffic (which contains the site-visit requests) through government-issued filtering boxes developed by software companies inside Iran. The boxes work by searching for banned text strings—either keywords or domain names—in the URL requests submitted by users.

In recent years there has been pressure within the Iranian government to show that the filtering of content is based on a legal framework and is not arbitrary. As a result, institutions in charge of internet filtering have evolved. In July 2009, Ahmadinejad's government enacted the Computer Crime Law, which had been passed by the parliament a year earlier. According to this law, the Committee in Charge of Determining Unauthorized Websites is legally empowered to identify sites that carry forbidden content and report that information to TCI and other major ISPs for blocking. The committee is headed by the prosecutor general and operates under the supervision of his office. The rest of the panel consists of representatives from 12 governmental ministries and institutes. The law also identifies the violations that might result in a website being marked for filtering. These are

defined very broadly and cover a variety of topics, ranging from insulting religious figures and government officials to distributing pornographic content and illegal circumvention tools.

Little information is available about the inner workings of the committee. According to the law it should meet biweekly to decide on any website bans, but a TCI vice president recently put the rate of filtering at 200 to 300 websites per day, meaning the bulk of filtering decisions are likely made automatically upon discovery of objectionable content, or by a small technical group in charge. This would leave the committee to decide on only the more controversial blocking decisions, such as the move during the protests to block the website of the Combatant Clergy Association (Majmae Rohanion Mobarez), a pragmatic-conservative clerical party linked to Rafsanjani. The official websites of Khatami and a number of Grand Ayatollahs who have criticized the government were also blocked. As the head of two important state bodies, the former president remained an influential member of the establishment, but he had been Ahmadinejad's electoral opponent in 2005, and he sometimes appeared to side with the opposition in 2009.

There have been other cases of filtering aimed at websites that operate within the official discourse. A number of websites and blogs belonging to Ahmadinejad supporters who publicly criticized some of his government's policies were also blocked. In such an environment, any website that includes elements of opposition discourse is bound to be targeted. The opposition Green Movement, other political groups, women's rights groups, ethnic and religious minorities, and the Iranian homosexual community fall within the category of opposition discourse and are affected by heavy filtering. In addition to blocking certain content, the Computer Crime Law makes service providers, such as blogging platforms, responsible for any content that appears on their sites. This has led to the suspension of a number of blogs hosted on platforms inside Iran.

The authorities claim that there is a procedure for disputing filtering decisions. However, the procedure is highly inefficient, even for a prominent conservative blogger, Omid Hosseini-Ahestan, whose site was filtered "accidentally." He did not succeed in unblocking his blog through the complaint procedure, but the filter was lifted after high-profile media coverage of the incident.[7] The dispute process requires the website owner to disclose his or her personal information and accept responsibility for any misconduct in the future, a commitment that few are willing to make given the risk of severe punishment.

In addition to censorship, the state counters critical content and online organizing efforts by extending state propaganda into the digital sphere. There are at least 400 news websites that are either directly or indirectly supported by the state. They seek to set the agenda by providing partial commentary or publishing rumors. There have also been a large number of government-backed initiatives to promote blogging among supporters of

[7] Ahestan blog, "On filtering of Ahestan", January 15, 2010. http://ahestan.wordpress.com/2010/01/15/ahestan.

government and members of the Basij paramilitary group. And during the postelection protests, there were reports of fake user-generated content submitted to Twitter and YouTube by government supporters to mislead the protesters and reporters. Some commentators have argued that propaganda is displacing censorship as the primary means of controlling the internet.[8]

Self-censorship is also very extensive, particularly on political matters. The widespread arrests of reporters and activists after the election, as well as perceptions of pervasive surveillance, have created fear among online journalists and bloggers. Many of them either abandoned their online activities or were forced to use pseudonyms. At least 1,500 bloggers who were blogging on political issues with their real identity decided to end their blogs or avoid writing about politics directly in the aftermath of the 2009 election. Furthermore, the majority of independent content producers lack the financial resources to operate in such a hostile environment. The online advertising market in Iran is exclusively limited to apolitical and pro-government websites. Even businesses based outside Iran avoid political websites to maintain trading relationships with the country. Due to international sanctions against Iran, Google Advertising does not recognize Persian as one of the languages in its advertising system, disadvantaging Persian content producers.

Despite all of these limitations, the internet remains the only means available for Iranian citizens and dissenters to get news and organize themselves. Iranian broadcast outlets are tightly controlled by the authorities, and satellite broadcasting from outside Iran is subjected to heavy jamming. The technical difficulty of engaging in similarly comprehensive censorship of a medium as complex and heavily populated as the Iranian internet may explain the authorities' growing reliance on propaganda, misinformation, and physical coercion to counter internet-based activism.

VIOLATIONS OF USER RIGHTS

Iranian internet users suffer from routine surveillance, harassment, and the threat of imprisonment for their online activities, particularly those who are more critical of the authorities. The constitution provides for limited freedom of opinion and expression, but numerous, haphazardly enforced laws restrict these rights in practice. The 2000 Press Law, for example, forbids the publication of ideas that are contrary to Islamic principles or detrimental to public rights, none of which are clearly defined. The government and judiciary regularly invoke this and other vaguely worded legislation to criminalize critical opinions. The Computer Crime Law passed by the parliament in 2008 and introduced

[8] Evgeny Morozov, "Iran's Propaganda Hits the 'Spinternet,'" CNN, December 29, 2009, http://edition.cnn.com/2009/OPINION/12/29/morozov.dicatorships.internet/index.html.

officially by Ahmadinejad in July 2009 clearly identifies punishments for spying, hacking, piracy, phishing, libel, and publishing materials that are immoral and against public taste.

Since June 2009 the authorities have been cracking down on online activism through various forms of judicial and extrajudicial intimidation. An increasing number of bloggers have been threatened, arrested, tortured, kept in solitary confinement, and denied medical care, while others have been formally tried and convicted. At least 50 bloggers and online activists have been arrested, and a dozen are still being detained. They include 18-year-old Navid Mohebbi, who was arrested in September 2010 and then released conditionally in December after receiving a three-year suspended prison sentence on charges of "actions against national security" and insulting the Islamic Republic's founder and current leader by means of "foreign media." Another blogger Omidreza Mirsayafi died under questionable circumstances in Tehran's infamous Evin prison. He was arrested in the aftermath of the election for allegedly insulting Iran's religious leaders and conspiring against the government. A large number of bloggers, journalists, and activists have also fled Iran and sought political asylum in neighboring countries, mainly Turkey.

The Iranian authorities have taken a range of measures to monitor online communications and use them as a basis for criminal punishment. A number of protesters who were put on trial after the election were indicted for their activities on Facebook and Balatarin, a Persian site that allows users to share links and news. Many arrested activists reported that interrogators had confronted them with copies of their e-mails, asked them to provide the passwords to their Facebook accounts, and questioned them extensively on their relationships with individuals on their "friends" list. The authorities actively exploited the fear created by these reports, claiming that they had access to all the e-mail and text messages exchanged in Iran. The Computer Crime Law obliges ISPs to record all the data exchanged by their users for a period of six months, but it is not clear whether the security services have the technical ability to monitor all this data. In addition, ISPs have been accused of forging SSL certificates to eavesdrop on emails sent through secure channels (https), making protected communication increasingly difficult for those without more sophisticated skills.

Explicit filtering and physical intimidation is supplemented by hacking and denial-of-service (DoS) attacks on the websites of government critics, including leading opposition figures. In the days after the disputed presidential election, many of the news websites set up by supporters of opposition candidates Mir Hossein Mousavi and Mehdi Karoubi were taken offline through arrests of the technical teams involved in their maintenance and through intense DOS attacks. There is technical evidence, including a log of the web servers, confirming that government-owned internet-protocol (IP) addresses were used to launch attacks on opposition websites.[9]

[9] Norooz News, "Norooz is revealing the names of 4 governmental entities behind the attacks against reformist websites," October 17, 2010.

Websites were rendered either permanently or temporarily unavailable by means of hacking. A group calling itself the Iranian Cyber Army managed to hack a number of opposition and news sites with a mix of technical methods and forgery. In some cases the hacking resulted in total discontinuity of the websites. One outlet so affected was MowjCamp.com, a popular site launched after the election that very soon became the main news website of the Green Movement. Outlets that were temporarily disabled by hacking included the Amsterdam-based Radio Zamaneh and the Jaras Green Movement website. A number of non-Iranian sites, such as Twitter, were targeted through the temporary hijacking of their domain names. At the time of these hacking incidents, there was speculation about the connection between the Iranian Cyber Army and the Iranian authorities. Some months later, Iranian officials confirmed these suspicions by publicly announcing that the Iranian Cyber Army was under the command of the IRGC.[10]

[10] Fars News, "IRGC has formed the second cyber army in the world," May 20, 2010, http://www.farsnews.com/newstext.php?nn=8902300353.

ITALY

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Free**
Obstacles to Access	n/a	6
Limits on Content	n/a	8
Violations of User Rights	n/a	12
Total	**n/a**	**26**

POPULATION: 60.5 million
INTERNET PENETRATION: 49 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Italy has a relatively high internet penetration rate, with about 50 percent of the population accessing the medium in 2009. Mobile-telephone usage is ubiquitous, and internet access via mobile phones has grown significantly in recent years. Italian authorities do not engage in political censorship of online speech, and no bloggers were imprisoned as of the end of 2010. However, in recent years the government has introduced several bills or decrees that could pose serious challenges to freedom of expression online, and a number of controversial judicial decisions have reinforced this trend. Freedom of expression advocates have raised concerns over efforts to make websites responsible for prescreening information, particularly videos, posted by their users, as well as attempts to impose onerous registration and other requirements on online communications. By the end of 2010, many of these worrisome proposals had been abandoned or put on hold.

The push to restrict internet freedom stems in part from the media ownership structure in Italy. Prime Minister Silvio Berlusconi owns, directly and indirectly, a large private media conglomerate, and his political position gives him significant influence over the appointment of state television officials. Such financial and editorial dominance of the broadcast media may give the country's leadership an incentive to restrict the free flow of information online, whether for political reasons or to influence the competition for viewers arising from online video. Nevertheless, as of the end of 2010, the diversity of views and degree of government criticism in online discussions was largely unrestricted and appeared to be greater than in the broadcast and print media.

A group of nuclear physicists created Italy's first computer network in 1980, with the intent of connecting all nuclear research institutes in the country. At the beginning, the internet was just one of several packet-switching networks that coexisted in Italy. The dominant telecommunications firm at the time, Telecom Italia, tried to impose its privately owned system, while various center-left governments, aware of the importance of interconnectivity, supported integration among the networks. Ultimately, the adaptability and simplicity of the internet prevailed. Access to the internet was available to private users after 1995, and the number of internet-service providers (ISPs) soared within a short period of time. Early obstacles to penetration included lack of familiarity with computers and with the English language, as well as the dominance of commercial television and the diversion of consumers' telecommunications spending to mobile telephony.

OBSTACLES TO ACCESS

Since 1990, the Italian government has supported the internet as a catalyst for economic growth, increased tourism, reduced communication costs, and more efficient government operations. As of 2009, Italy had approximately 29 million internet users, for an internet penetration rate of almost 50 percent.[1] Although this rate is higher than the global average, it is lower than the overall penetration rate in Western Europe. The relatively low penetration rate is not due to infrastructural limitations as much as unfamiliarity with the internet among the older generations and a general affinity for mobile-phone devices rather than desktop computers.

The main point of internet access is the home, with approximately 18 million people using home connections at least once a month.[2] The workplace is the second most common access point, with approximately 6 million users, followed by schools and universities, with around 2 million users. Approximately 43 percent of internet users are female, but women make up 55 percent of "new users."[3] Cost is not a significant barrier to access. Currently, the price for a broadband connection ranges from €20 to €40 (US$26 to US$52) per month.[4]

ADSL broadband connections are available on 86 percent of Italy's territory.[5] However, the broadband subscription rate is only 20.5 percent, as not all internet

[1] International Telecommunication Union (ITU), "ICT Indicators 2009—Internet," available at http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx, accessed March 2, 2011.
[2] Giancarlo Livraghi, ed., "Dati sull'internet in Italia" [Data on the Internet in Italy], as of December 24, 2010, http://www.gandalf.it/dati/dati3.htm (in Italian).
[3] Ibid.
[4] "Broadband—Italy," Socialtext, https://www.socialtext.net/broadband/index.cgi?italy, accessed March 4, 2011.
[5] Ibid.

subscribers opt for higher speeds.[6] Meanwhile, fiber-optic cables are not well developed. In September 2010, the deputy minister for communications announced that Italian telecommunications operators had reached an agreement on the technical model for a transition from the existing copper-wire network to a fiber-optic network. Earlier in the year, telecommunications operators Fastweb, Wind, and Vodafone Italia had announced plans to jointly invest €2.5 billion (US$3.3 billion) over a five-year period to connect 15 of Italy's largest cities using fiber-optic cable, and cover an additional 10 million people. Telecom Italia has announced its own plan to invest €9 billion (US$11.8 billion) in infrastructure, and aims to offer 100 Mbps broadband access to 50 percent of the Italian population by 2018.[7]

In terms of mobile-phone penetration, Italy leads Organization for Economic Cooperation and Development (OECD) countries with a rate of 151 percent.[8] The majority of these subscriptions are prepaid. Telecom Italia Mobile (TIM), Vodafone, Wind, and 3 Italia are the major carriers, and all of them operate third-generation (3G) networks. Access to mobile internet has been increasing in recent years, and as of December 2009, some 9 percent of internet users reported accessing the internet through their mobile phones.[9] The social-networking site Facebook, the Twitter microblogging service, and international blog-hosting sites are freely available. The popularity of videoconferencing through applications like Skype is on the rise.

In 2005, the Italian government issued the Pisanu decree, requiring businesses to obtain a license from the police in order to offer WiFi access to customers. The decree also required that users produce identification documents to access WiFi in public places, and that operators preserve a record of internet use. These measures were instituted for security reasons in the wake of terrorist bombings in London that year, and were renewed annually over the next several years. They are widely viewed as having stunted the spread of WiFi in Italy, as many businesses chose not to offer such services given the added nuisance and cost involved in complying with the decree. In November 2010, however, the government announced that it would abolish the decree and remove restrictions on public access to WiFi starting in January 2011. The government passed a decree to formalize the announcement in December 2010, but this required parliamentary approval within two months or the

[6] Google Public Data, "Broadband Penetration Rate: Italy," updated February 10, 2011, http://www.google.com/publicdata?ds=f5nrd26mp6q4m_&ctype=l&strail=false&nselm=h&met_y=broadband_penetration&scale_y=lin&ind_y=false&rdim=country_group&idim=eu_country:IT&tstart=1025481600000&tunit=M&tlen=90&hl=en&dl=en.

[7] Giada Zampano, "Italy Operators Reach Broadband Deal," *Wall Street Journal*, September 19, 2010, http://online.wsj.com/article/SB10001424052748703470904575499432808468868.html.

[8] Organization for Economic Cooperation and Development (OECD), "OECD Key ITC Indicators—Mobile subscribers in total / per 100 inhabitants for OECD, 2007," updated September 21, 2009, available at http://www.oecd.org/sti/ICTindicators.

[9] "ITALIA: accesso a Internet per luoghi e device (Dicembre 2009)" [Italy: Access to the Internet by Location and Device (December 2009)], Key4biz, March 4, 2010, http://www.key4biz.it/Figure_e_Tabelle/2010/03/Internet_Device_Web_Contenuti_Smartphone_Accesso_Utenti_Luoghi_Dicembre_Italia.html (in Italian).

previous requirements would remain in force. While many politicians welcomed the change, others were skeptical about whether the announcement would be followed by concrete action.[10]

Access to the internet for private users is offered by 13 different internet-service providers (ISPs). Telecom Italia has the largest share of the market, followed by Vodafone, Fastweb, and Tiscali.[11] Telecom Italia owns the physical network, but it is required by European Union (EU) legislation to provide fair access to competitors.[12]

The main regulatory body for telecommunications is the Authority for Communications Security (AGCOM), an independent agency that is accountable to Parliament. Its responsibilities include providing access to networks, protecting intellectual-property rights, regulating advertising, and overseeing public broadcasting. AGCOM's president is appointed by the majority party in Parliament and commissioners have been known to come under pressure from the government to take certain actions regarding television broadcasts.[13] The other important player in the field of communications is the Italian Data Protection Authority (DPA). Set up in 1997, the DPA has a staff of more than 100 people, and four of its main members are elected by Parliament for seven-year terms. The DPA is tasked with supervising compliance by both governmental and nongovernmental entities with data protection laws, and "banning or blocking processing operations that are liable to cause serious harm to individuals."[14] It is generally viewed as professional and fair in carrying out its duties.

LIMITS ON CONTENT

The Italian authorities engage in some blocking of internet sites, though to date there have been no known restrictions on politically oriented content, and Italians have access to the websites of a wide range of domestic and international news sources and human rights groups. Since 2006, online gambling has been permitted only via state-licensed websites, and ISPs are required to block access to international or unlicensed gambling sites identified on a blacklist compiled by the Autonomous Administration of State Monopolies (AAMS).

[10] Philip Willan, "Italy to Remove Public WiFi Restrictions," *Network World*, November 5, 2010, http://www.networkworld.com/news/2010/110510-italy-to-remove-public-wi-fi.html; Luca Annunziata, "Addio Pisanu, o arrivederci? (update 2)" [Farewell Pisanu, or See You Soon? (update 2)], *Punto Informatico*, December 22, 2010, http://punto-informatico.it/3061069/PI/News/addio-pisanu-arrivederci-update-2.aspx (in Italian).

[11] Telecom Italia, "Domestic Market," updated August 9, 2010, http://www.telecomitalia.com/tit/en/corporate/investors/business_areas_competitive_scenario/domestic_market.html.

[12] Lorenzo Pupillo, *Duct and Pole Sharing: An Operator's Perspective* (Rome: Telecom Italia, April 10, 2008), slide 14, http://www.oecd.org/dataoecd/35/61/40460866.pdf.

[13] Michael Day, "Silvio Berlusconi caught out trying to stifle media," *The Independent,* March 18, 2010, http://www.independent.co.uk/news/world/europe/berlusconi-caught-out-trying-to-stifle-media-1923147.html .

[14] Data Protection Authority, "The Italian Data Protection Authority: Who We Are," November 17, 2009, http://www.garanteprivacy.it/garante/doc.jsp?ID=1669109.

The list of banned sites is available on the AAMS website and updated regularly.[15] A similar blacklist system is in place for websites containing child pornography. A law passed in February 2006 (Law No. 6) called for the establishment of a National Center for the Fight against Child Pornography on the Internet within the Postal and Communications Police Service. Based on its own research and on complaints from citizens, the center maintains a list of sites deemed inappropriate and forwards it to ISPs for blocking.[16] As with the AAMS list, the child pornography blacklist is publicly available, though some child advocates have raised concerns that this encourages visits to the sites by users with circumvention tools. ISPs also offer subscribers "family internet" packages that block access to adult pornography and sites with violent content, in exchange for a small premium.

In addition to blocking entire websites, Italian authorities have issued formal requests for the removal of specific content. Overall, Italy ranked sixth in a list of countries published by Google based on the number of official requests for content removal. It issued 69 requests between January 2010 and June 2010, resulting in the removal of 1,655 items (or 97 percent of those requested), the vast majority of which had been posted on YouTube. The Google list did not explain the justifications for the requests,[17] though presumably they would have included child pornography and copyright infringement.

More worrying to free expression advocates have been judicial decisions that potentially extend registration requirements to blogs, or that appear to hold websites liable for content posted by users. Government attempts to introduce legislation that would require websites to engage in prepublication censorship have also raised concerns. In the face of public criticism, however, self-censorship requirements for ISPs and content providers had not been enacted as of the end of 2010.

The registration issue stems from a 1948 law against the "clandestine press." Drawing on that law, a regulation issued in 2001[18] holds that anyone who wants to provide a news service, including on the internet, must be a "registered" journalist in the Communication Workers' Registry (ROC), with membership in the national journalists' association. The rules have generally not been applied to bloggers, and in practice millions of blogs are published in Italy without repercussions. However, in September 2008, a judge in Sicily found local author Carlo Ruta guilty of publishing a "clandestine newspaper" in the form of a blog, which in this case contained detailed research on connections between politicians and organized crime. Ruta was fined €250 and forced to take down his blog, though he replaced

[15] The blacklist is available (in Italian) at http://www.aams.gov.it/site.php?id=2484.
[16] State Police, "Centro nazionale per il contrasto alla pedopornografia sulla rete" [National Center for the Fight against Child Pornography on the Internet], March 10, 2010, http://www.poliziadistato.it/articolo/view/10232/ (in Italian).
[17] Google, "Transparency Report: Government Requests," http://www.google.com/transparencyreport/governmentrequests/; Ed Felten, "Google Publishes Data on Government Data and Takedown Requests," *Freedom to Tinker* (blog), April 20, 2010, http://www.freedom-to-tinker.com/blog/felten/google-publishes-data-government-data-and-takedown-requests.
[18] Law No. 62, March 7, 2001, "Nuove norme sull'editoria e sui prodotti editoriali" [New Rules on Publishing and Publishing Products], available at http://www.interlex.it/testi/l01_62.htm.

it with a message linking visitors to his new website.[19] While the law is rarely applied in this way, many people who create websites on a range of issues, including scholarly research on foreign policy, collaborate with registered journalists to protect themselves from potential legal action.[20]

The apparent push to hold ISPs and websites responsible for user-posted content has been manifested in several separate incidents in recent years. Perhaps the most prominent case in this regard involved a 2006 video that was uploaded to Google Video, a video-sharing site operated by Google before it acquired YouTube. The video clip showed a mentally disabled child being bullied by his classmates. Although it remained online for two months and became quite popular, Google administrators removed it shortly after they were notified. Nevertheless, the city of Milan and the advocacy group Vivi Down sued four top Google executives for defamation and violation of the privacy protection law. In Italy, executives may be held legally responsible for a company's actions, and the privacy law prohibits the use of someone else's personal information to do them harm or make a profit. In February 2010, a judge found that the video was obviously posted without the victim's permission, and that Google was profiting from the resulting site traffic through online advertisements. The court sentenced three of the four executives to suspended six-month jail sentences, and acquitted them on the defamation charges. Freedom of expression advocates criticized the ruling, arguing that it effectively required websites to carry out prepublication screening of videos, a costly exercise that would open the door to abuse.[21] However, given that Italy has a civil-law rather than a common-law system, and that inconsistent judicial interpretations are not unusual, it remains unclear whether the Google decision will set a significant precedent.[22]

Also in early 2010, the government signaled its intention to extend television broadcasting regulations to websites that host videos.[23] The new rules, known as the Romani decree, were first proposed in January 2010. The initial draft required all websites showing videos—including blogs, online news outlets, and video-sharing websites—to first obtain a license from the government, and subjected them to fines of up to €150,000 in the event of copyright infringement.[24] This would effectively require websites to monitor all uploaded

[19] John Ozimek, "How an Italian Judge Made the Internet Illegal," *Register*, September 26, 2008, http://www.theregister.co.uk/2008/09/26/italian_law_kills_blog/.
[20] Interview with Luca Bolognini, president of the Italian Institute for Privacy, June 22, 2010.
[21] Reporters Without Borders, "Google Conviction Could Lead to Prior Control over Videos Posted Online, Says RSF," International Freedom of Expression eXchange (IFEX), February 25, 2010, http://www.ifex.org/italy/2010/02/25/google_conviction/; Elisabetta Povoledo, "Italian Judge Cites Profit as Justifying a Google Conviction," *New York Times*, April 12, 2010, http://www.nytimes.com/2010/04/13/business/global/13google.html.
[22] Manlio Cammarata, "Google–Vivi Down, una sentenza da cancellare" [Google–Vivi Down, A Sentence To Be Deleted], InterLex, April 14, 2010, http://www.interlex.it/675/google2.htm (in Italian).
[23] Stacy Meichtry and Giada Zampano, "Italy Set to Extend TV Rules to Web Videos," *Wall Street Journal*, February 3, 2010, http://online.wsj.com/article/SB10001424052748703338504575041401049214106.html.
[24] Reporters Without Borders, "Proposed Decree Would Require Websites Showing Videos to Obtain License," IFEX, January 21, 2010, http://www.ifex.org/italy/2010/01/21/video_licence/.

content, coming in some cases from millions of users. Following a public outcry, the decree was amended to exclude blogs, video-sharing sites, and online news publications. However, websites providing video content or live streaming for profit, such as internet-protocol television (IPTV) services, would be covered. [25] They would be required to register with AGCOM and face a ceiling on advertisement. An early draft included some AGCOM oversight of content as well, and while this provision was later withdrawn by the government, some observers remained convinced that attempts to impose content censorship would come up again in the future. The revised decree passed at the end of March 2010.

Some critics have suggested that the Romani decree was motivated by Berlusconi's financial and political interest in maintaining the popularity of television versus online video.[26] In another apparent manifestation of this interest, Berlusconi's Mediaset conglomerate had sued Google's YouTube in July 2008 over user-posted clips from Mediaset-owned shows.[27] YouTube has a policy of promptly removing copyright-infringing content as soon as it is notified, but in December 2009 a Rome court ruled against the video-sharing site, holding it responsible for the violations of copyright.[28]

Even in the absence of legal requirements, ISPs tend to exercise some informal self-censorship, declining to host content that may prove controversial or that could create friction with powerful entities or individuals. Online writers also exercise caution to avoid libel suits by public officials, whose litigation—even when unsuccessful—often takes a significant financial toll on defendants in the traditional media. The Italian government does not proactively manipulate news websites. However, coverage in traditional media does affect what is published on news websites, giving the outlets controlled by the prime minister an indirect influence over online reporting.

Blogging has become popular in Italy, though television remains by far the leading medium for obtaining news. Most policymakers, popular journalists, and figures in the entertainment industry have their own blogs, as do many ordinary citizens. Social-networking sites, especially Facebook and Twitter, have emerged as crucial tools for

[25] Guido Scorza, "Decreto Romani, meglio ma non bene" [Romani Decree, Better But Not Good], *Punto Informatico*, March 2, 2010, http://punto-informatico.it/2823280/PI/Commenti/decreto-romani-meglio-ma-non-bene.aspx (in Italian).
[26] Jeff Israely, "Berlusconi vs. Google: Will Italy Censor YouTube?" *Time*, January 22, 2010, http://www.time.com/time/world/article/0,8599,1955569,00.html.
[27] Chiara Remondini, "Mediaset Sues Google, YouTube, Seeking EU500 Million (Update2)," Bloomberg, July 30, 2008, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aYyj.ATOyYDs.
[28] By contrast, a Spanish court, which also ruled on the case because the plaintiff was a Spanish subsidiary of Mediaset, rejected the demand for compensation, arguing that YouTube was only an "intermediary" and thus not responsible for the content. Moreover, the judge stated that specific takedown requests must be presented for each clip lest YouTube be forced to exercise prepublication content control. See Gaia Bottà, "YouTube, il Grande Fratello va asportato" [YouTube, Big Brother Should Be Removed], *Punto Informatico*, December 16, 2009, http://punto-informatico.it/2773039_2/PI/News/youtube-grande-fratello-va-asportato.aspx (in Italian); Mauro Vecchio, "YouTube, Mediaset incornata" [YouTube, Mediaset Goring], *Punto Informatico*, September 23, 2010, http://punto-informatico.it/2996681/PI/News/youtube-mediaset-incornata.aspx (in Italian); Ryan Lawler, "YouTube Loses Copyright Case in Italian Court," GigaOM, December 17, 2009, http://gigaom.com/video/youtube-loses-copyright-case-in-italian-court/.

organizing protests and other mass gatherings, such as concerts, parties, or political rallies. As of the end of 2010, Italy had about 17 million Facebook users. In December 2009, a "No Berlusconi Day" protest calling for the prime minister's resignation was organized by bloggers and publicized almost entirely over the internet and social-networking sites. It drew roughly 100,000 people.[29] In December 2010, students used the internet to organize a protest against a bill that substantially modified the structure of Italy's university system. Despite a large turnout, however, the bill was ultimately approved.[30] Separately, the surveillance potential of social-networking sites was highlighted in March 2010, when Facebook usage by a wanted organized crime suspect enabled police to locate and arrest him.[31]

Given the polarization and heated discourse in Italian politics, some content on social-networking platforms has been aggressive enough to potentially incite violence. In 2009, fan pages for imprisoned Mafia bosses emerged, as did a Facebook group called "Let's Kill Berlusconi."[32] The original creators of the group, which quickly grew to tens of thousands of followers, maintained that it was not to be taken at "face value," but was rather a provocation for those who were "fed up" with the premier.[33] In another case, a group was created in support of Massimo Tartaglia, a mentally ill man who struck Berlusconi with a statuette in December 2009, causing injuries to his teeth and nose; the Facebook fan page for Tartaglia gained nearly 100,000 followers in under 48 hours. Meanwhile, several other groups arose with the aim of defending the prime minister. The two "factions" went on denouncing each other on the web for some time. In response, Italian officials contacted Facebook, which ultimately decided to remove the groups.

VIOLATIONS OF USER RIGHTS

Freedoms of speech and the press are constitutionally guaranteed and generally respected despite ongoing concerns regarding concentration of media ownership, particularly Berlusconi's control over both public and private media assets.[34] The constitution also

[29] "Bloggers Organize 'No Berlusconi Day' Protest," France 24, December 5, 2009, http://www.france24.com/en/20091205-bloggers-silvio-no-berlusconi-day-protest-italy-prime-minister-corruption; Bernardo Parrella, "Italy: Online Activism Fires Up 'No Berlusconi Day,'" Global Voices, November 17, 2009, http://globalvoicesonline.org/2009/11/17/italy-online-activism-fires-up-no-berlusconi-day/. The movement's website can be found at http://www.noberlusconiday.org/.

[30] "Italian Students Demonstrate Against Education Reforms," British Broadcasting Corporation (BBC), December 22, 2010, http://www.bbc.co.uk/news/world-europe-12058434.

[31] Ann Wise, "Mafia Boss Betrayed by Facebook," American Broadcasting Company (ABC), March 17, 2010, http://abcnews.go.com/International/facebook-finds-mafia-boss/story?id=10124958&page=1.

[32] Eric Sylvers, "Facebook to Monitor Berlusconi Content," *New York Times*, December 15, 2009, http://www.nytimes.com/2009/12/16/technology/internet/16iht-face.html.

[33] "Probe Into 'Kill Berlusconi' Call," BBC, October 22, 2009, http://news.bbc.co.uk/2/hi/europe/8320333.stm.

[34] Karin Karlekar, ed., "Italy," in *Freedom of the Press 2010* (New York: Freedom House, 2010), http://www.freedomhouse.org/template.cfm?page=251&year=2010.

contains provisions protecting confidentiality of correspondence,[35] and Italy is a signatory to the European Convention on Human Rights and relevant international treaties. In recent years, the executive branch has been accused of trying to extend the control it wields over the television sector to the internet. This is partly because key individuals in the current government are very familiar with broadcast media, but surprisingly unfamiliar with the internet, including the prime minister and Vice Minister for Communications Paulo Romani.[36] Initial drafts of legislation introduced in recent years with the aim of regulating new media have drawn too heavily on the parallel with television, generating provisions that are inappropriate for the more interactive medium of the internet. For example, the draft version of the Romani decree, described above, would have crippled a range of websites with its heavy restrictions on video content.[37] However, after strong opposition by internet NGOs, users, and private business associations, the government amended the decree before final approval.

Defamation remains a criminal offense in Italy, punishable by prison terms ranging from six months to three years,[38] and a minimum fine of €516 (US$670).[39] In the case of libel through the press, television, or other public means, there is no prescribed maximum fine.[40] Though these provisions are rarely applied, civil libel suits against journalists are a common occurrence, including by public officials. In 2009, the prime minister sued multiple domestic and international media companies, accusing them of defaming him through their coverage of his private life.[41] Although 8 out of 10 defamation cases are reportedly decided in favor of the journalists, the financial burden of lengthy legal

[35] An English copy of the constitution is available at http://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf. See especially Articles 15 and 21.

[36] The prime minister's mispronunciation of Google's name during a press conference was seen as a sign of unfamiliarity with the basics of the internet. See "Berlusconi inciampa su Google;
E chiama 'Gogol' il motore di ricerca" [Berlusconi Trips Over Google; The Search Engine Is Called 'Gogol'], *Il Corriere della Sera*, May 20, 2010, http://www.corriere.it/politica/10_maggio_19/berlusconi-google-gogol_db608a2c-6346-11df-8b63-00144f02aabe.shtml (in Italian). Romani is a former freelance journalist with a background that is heavily skewed toward broadcasting and television.

[37] Giorgio Pontico, "In Italia Internet arranca" [In Italy Internet Limps], *Punto Informatico*, April 1, 2010, http://punto-informatico.it/2846003/PI/News/italia-internet-arranca.aspx (in Italian).

[38] Dana Kennedy, "Knox's Parents Are Just the Latest to Run Afoul of Italy's Libel Laws," AOL News, February 16, 2011, http://www.aolnews.com/2011/02/16/amanda-knoxs-parents-are-just-the-latest-to-run-afoul-of-italy/.

[39] Organization for Security and Cooperation in Europe (OSCE) Representative on Freedom of the Media, *Libel and Insult Laws: A Matrix on Where We Stand and What We Would Like to Achieve* (Vienna: OSCE, 2005), 79, http://www.osce.org/fom/41958.

[40] Ibid.

[41] Javier Espinoza, "Berlusconi's Libel Lawsuits," *Forbes*, August 28, 2009, http://www.forbes.com/2009/08/28/berlusconi-legal-action-markets-equities-libel.html; "Tg1, Minzolini attacca la manifestazione: 'Libertà di stampa in pericolo? Assurdo'" [Tg1, Minzolini Attacks the Event: 'Freedom of the Press in Danger? Absurd'], *La Repubblica*, October 3, 2009, http://www.repubblica.it/2009/10/sezioni/politica/liberta-stampa-2/minzolini-editoriale/minzolini-editoriale.html (in Italian). See also, for example, "Fini querela il Giornale: delirio diffamatorio. Ma il quotidiano conferma il nuovo affondo" [Fini il Giornale Complaint: Defamatory Delerium. But the Daily Confirms the New Thrust], *Il Sole 24 Ore*, August 13, 2010, http://www.ilsole24ore.com/art/notizie/2010-08-13/fini-querela-giornale-casa-114119.shtml (in Italian); Paolo Bracalini, "Grillo e Di Pietro contro le querele. Degli altri" [Grillo and Di Pietro Against Lawsuits. Of Others], *Il Giornale*, August 13, 2009, http://www.ilgiornale.it/interni/grillo_e_di_pietro_contro_querele_degli_altri/13-08-2009/articolo-id=373848-page=0-comments=1 (in Italian).

proceedings produces a chilling effect. Libel suits against bloggers and other online writers remain relatively rare. However, in May 2006, blogger Roberto Mancini was convicted of defamation and instructed to pay a fine of €13,500 (US$17,500). Using the pseudonym General Sukhov, Mancini had apparently posted several articles on his blog that criticized local figures. Reporters Without Borders claimed that Mancini was punished not only for using "bad language" in his posts, but also for comments posted on the blog by his readers.[42]

In early 2010, a draft law commonly known as the wiretap bill was introduced in Parliament by Justice Minister Angelino Alfano. The bill's proponents said it aimed to address concerns over the right to privacy and the problem of news media regularly publicizing wiretap information that is leaked to them. However, several provisions appeared to threaten media freedom and the right of the public to access independent information. Though it primarily applied to traditional media, aspects of the proposal would also affect online media. For example, accredited journalists who recorded or filmed an individual without his or her permission would face fines of up to €10,000 (US$13,000) and as many as 30 days in jail, and other individuals who violated the rule, potentially including citizen journalists and bloggers, could be fined up to €464,700 (US$602,600) and spend as much as four years in prison. Another provision would restrict the publication of documents related to court proceedings or police investigations prior to the beginning of a trial. The release of leaked wiretap information would lead to heavy financial penalties for publishers and jail for journalists. The bill would also oblige websites, like print publications, to issue corrections within 48 hours of receiving notice of an error, or risk a fine of up to €25,000 (US$32,000). That provision would apply to any "information websites," in addition to online news outlets.[43] The legislation's treatment of online platforms, including blogs, in a similar manner to print media could result in a requirement that they legally register as newspapers do.[44]

In June 2010, the bill was adopted by the Chamber of Deputies and the Senate, which made amendments and returned it to the lower chamber. Both the Organization for Security and Cooperation in Europe's representative on freedom of the media and the UN special rapporteur on freedom of expression called on Italy to drop the wiretap bill or revise it to bring it in line with international standards.[45] In the wake of such international criticism

[42] Reporters Without Borders, "A Blogger Unfairly Convicted of Defamation," news release, June 20, 2006, http://en.rsf.org/italy-a-blogger-unfairly-convicted-of-20-06-2006,18068.html.
[43] Arianna Ciccone, "Italy: Liability Risk for Bloggers?" Global Voices Advocacy, July 27, 2010, http://advocacy.globalvoicesonline.org/2010/07/27/italy-a-bill-to-censor-the-internet/.
[44] Barbara Trionfi and Anthony Mills, *Press Freedom in Italy: Between Political Influence & Conflicts of Interest* (Vienna: International Press Institute, 2010), http://www.freemedia.at/fileadmin/media/Documents/IPI_mission_reports/Italy_Mission_Report_2010_FINAL.pdf.
[45] OSCE Representative on Freedom of the Media, "OSCE Media Freedom Representative Urges Italy to Amend Bill on Electronic Surveillance," news release, June 15, 2010, http://www.osce.org/fom/69428.

as well as advocacy by local groups, the bill had reportedly been put on hold as of November 2010.[46]

Monitoring of personal communications is permissible only if a judicial warrant has been issued, and widespread technical surveillance is not a concern in Italy. Nevertheless, the country's authorities are known for engaging in a large number of wiretaps.[47] According to 2006 figures from the German think-tank the Max Planck Institute, Italy leads the world in terms of wiretaps, with 76 intercepts per 100,000 people.[48] By other official estimates, roughly 100,000 wiretaps are carried out each year.[49] Wiretapping is generally restricted to cases involving ongoing legal proceedings, except for terrorism investigations. In such instances, since 2001, "pre-emptive wiretapping" may occur even if no formal prosecutorial investigation has been initiated. More lenient procedures are also in place for Mafia-related investigations.[50]

In March 2008, Parliament approved a law (No. 48 of 2008) that ratified the Council of Europe's Convention on Cybercrime, which established how long internet-related communication data should be retained.[51] This matter was further refined with the inclusion in the Italian legislative system of the 2006 EU Data Retention Directive.[52] Under the current legal framework, ISPs must keep users' traffic records—though not the content of communications—for 12 months. This includes broadband internet data, internet telephony, internet use via mobile phone, and e-mail activity.[53] The records can only be disclosed in response to a request from a public prosecutor (a judge) or a defendant's lawyer, and, like their counterparts elsewhere in Europe, Italy's law enforcement agencies may ask ISPs to make such information readily available so that they can respond to the needs of criminal investigations. Given the technical burden of this directive, most ISPs now

[46] Trionfi and Mills, *Press Freedom in Italy*.

[47] Although it is difficult to determine the real number of people affected by wiretaps (estimates range from 25,000 to over 130,000), many individuals who are caught up in wiretaps have no incriminating connection to the main target of the eavesdropping. The current law stipulates that such peripheral communications cannot be transcribed and any recordings should be destroyed right away, though this is not always carried out in practice. Thus it may happen that some exchanges are recorded and leaked to the media. This is the problem that the proposed bill on electronic surveillance was meant to address. See for example Cristina Bassi, "Intercettazioni, quante sono e quanto costano" [Interceptions, How Many and How Much They Cost], Sky TG24, June 13, 2010, http://tg24.sky.it/tg24/cronaca/2010/06/12/intercettazioni_quante_sono_e_quanto_costano.html (in Italian).

[48] Duncan Kennedy, "Italian bill to limit wiretaps draws fire," BBC, June 11, 2010, http://www.bbc.co.uk/news/10279312.

[49] Trionfi and Mills, *Press Freedom in Italy*, 19.

[50] Privacy International, "Italy: Privacy Profile," in *European Privacy and Human Rights 2010* (London: Privacy International, 2010), https://www.privacyinternational.org/article/italy-privacy-profile.

[51] For a useful timetable of the required retention periods, see Gloria Marcoccio, "Convention on cybercrime: novità per la conservazione dei dati" [Convention on Cybercrime: News on Data Retention], InterLex, April 10, 2008, http://www.interlex.it/675/marcoccio7.htm (in Italian). See also Andrea Monti, "Data Retention in Italy. The State of the Art," *Digital Thought* (blog), May 30, 2008, http://blog.andreamonti.eu/?p=74.

[52] Legislative Decree No. 109, May 30, 2008.

[53] Privacy International, "Italy: Privacy Profile," in *European Privacy and Human Rights 2010* (London: Privacy International, 2010), https://www.privacyinternational.org/article/italy-privacy-profile.

use a third-party service that offers the necessary security guarantees for encryption and data storage.

There have been no reports of extrajudicial intimidation or physical violence in response to online activity, though individuals directly exposing the activities of organized crime in some parts of the country may be at risk of reprisals. Defacement of websites for political reasons does occur, but it is rare. More serious cyberattacks—particularly against banks, government institutions, and business websites—are a problem in Italy, as in other EU member states. Moreover, Italy ranks high on the list of countries identified as points of origin for cybercrimes. The law enforcement agency with primary responsibility for cybercrimes is the Postal and Communications Police Service. Police officers are primarily concerned with cybercrime in the form of child pornography, cyberbullying, and various forms of fraud.[54] A special branch within the service, the National Center for Infrastructure Protection, is tasked with the protection of the country's critical infrastructure.[55]

[54] Figures on cybercrime are difficult to assess, as the main providers of data are computer security companies such as Symantec or government entities like the postal police, as opposed to "third-party" sources. Nevertheless, Italy's rates appear to be slightly above the world average. See Tiziana Moriconi, "Crimini online, i dati italiani" [Online Crime, the Italian Data], *Daily Wired*, November 23, 2010, http://daily.wired.it/news/internet/hacking-accordo-tra-symantec-e-polizia-postale.html (in Italian); Alessandra Talarico, "Cybercrime. Italia vittima e carnefice: è il paese che più abbocca al phishing e tra i più attivi negli attacchi web based" [Cybercrime. Italy Victim and Victimizer: It Is the Country That Takes the Bait in Phishing and Is Among the Most Active in Web-Based Attacks], Key4Biz, April 22, 2010, http://www.key4biz.it/News/2010/04/22/eSecurity/cybercrime_botnet_spam_ebanking_social_network_spyware_adware_phishing.html (in Italian). For a recognition of the professionalism of Italy's postal police, see Alessandra Talarico, "Lotta al cybercrime: avrà sede a Roma nuova task force Usa-Europa. Utilizzerà le tecnologie di Poste Italiane" [Fighting Cybercrime: A New U.S.-European Task Force Will Be Based in Rome. Will Use the Technologies of the Italian Post], Key4Biz, June 30, 2009, http://www.key4biz.it/News/2009/06/30/eSecurity/cybercrime_sicurezza_reti_European_Electronic_Crime_Task_Force_US_Secret_Service_Massimo_Sarmi.html (in Italian).

[55] Critical infrastructure includes telecommunications networks, energy and water distribution systems, banking networks, and transportation and emergency services.

JORDAN

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Partly Free**
Obstacles to Access	n/a	12
Limits on Content	n/a	11
Violations of User Rights	n/a	19
Total	**n/a**	**42**

POPULATION: 6.5 million
INTERNET PENETRATION: 28 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Jordan, a small kingdom of about six million people, prides itself on offering relatively broad freedom to use the internet and officially blocks only one website. Nonetheless, internet users are aware that their browsing history, comments, and posted materials may be monitored by the authorities. The government's appreciation of this unique access to public opinions and reactions seemed to have outweighed, until recently, its impulses to control content and limit expression online. However, the new law on cybercrimes, adopted in August 2010, contains several provisions that could be used to limit free expression on the internet, provoking vehement protests by web publishers and internet activists. The government had threatened earlier to introduce legislation covering internet use, but journalists and news website owners had pushed back, arguing that online material is already tempered by the self-censorship to which Jordanians have grown accustomed. Nonetheless, the government imposed the restrictive law, prompting speculations within the web community about the effects of its implementation.

Internet access was first provided to Jordanians in 1995, and the Telecommunications Regulatory Commission (TRC) was created that year to oversee the medium.[1] The authorities quickly recognized the economic potential of the internet and actively promoted the development of information and communication technologies (ICTs) in the kingdom.[2] Groups and individuals can obtain internet access through privately owned

[1] The TRC was established as a financially and administratively independent jurisdictional body through the Telecommunications Law (No. 13 of 1995) and a subsequent amendment (Law No. 8 of 2002).
[2] Privacy International, "Jordan," in *Silenced: An International Report on Censorship and Control of the Internet* (London: Privacy International, 2003), http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-103564.

service providers, and no special state approval or registration is required, but traffic must still flow through the government telecommunications hub.[3] As the number of internet users began doubling and tripling each year, the government responded by stepping up both infrastructure expansion and monitoring. Although the authorities are aware of the need to develop the ICT sector for the country's survival and progress, they are nonetheless concerned about the information and the freedom that the internet can bring to the people.

OBSTACLES TO ACCESS

According to the International Telecommunication Union (ITU), there were 1,741,900 internet users in Jordan in 2009, representing about 27.6 percent of the population.[4] Most internet users are still young people ranging in age from 15 to 24,[5] but the medium, once seen as a tool for trivial entertainment and the exchange of scandalous or banned information, has grown into a vital instrument for business and an important forum for public discussion. About two-fifths of Jordanian families were reported to have personal computers as of early 2009, and the number of broadband subscribers reached 203,500 that year, up from just 24,000 at the end of 2005. Mobile-telephone use has also expanded rapidly; there were about 3.1 million subscribers in 2005, but by early 2010 the number of subscriptions had exceeded the total population.[6]

There are frequent government initiatives to encourage schools and universities to offer internet access. A program aimed at providing every student with a laptop computer is ongoing, and over 11,000 laptops have been sold to university students at discounted prices.[7] Other initiatives have focused on establishing and modernizing the infrastructure required to support ICT-assisted instruction. By 2009, 72 percent of learners were entitled to use internet laboratories at school as a pedagogical aid, and 80 percent of schools had internet-assisted instruction.[8]

Expansion of internet access has been hampered by the cost of computers and connectivity. For the past several years, internet connection fees were considered high in comparison with neighboring countries and with the cost of living. Prices have decreased reportedly upon direct orders from the king, but complaints about the level of service have

[3] Ibid.

[4] International Telecommunications Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#.

[5] Mohammad Ghazal, "Jordan, UAE Firms in Talks over Free IT Zone," *Jordan Times*, May 16, 2009, http://www.jordantimes.com/?news=16742.

[6] International Telecommunications Union (ITU), "ICT Statistics 2009—Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#; "Number of cellular subscribers in Jordan exceeds the number of inhabitants," Jordan Zad, November 21, 2009, http://www.jordanzad.com/jordan/print.php?a=27318.

[7] Ghazal, "Jordan, UAE Firms in Talks over Free IT Zone."

[8] ITU, "World Telecommunication Development Report" (Target 7), http://www.itu.int/ITU-D/ict/publications/wtdr_10/material/WTDR2010_Target7_e.pdf.

persisted. Monthly internet subscription prices currently range from 14 Jordanian Dinars (JD) (US$20) for the speed of 128 kilobytes per second (kbps) to about 30 JD (US$42) for the speed of up to 2 megabytes per second (mbps) for uploads and 10 mbps for downloads. These charges are often twice as much for subscriptions in an office setting. Clients often claim that connection speeds fluctuate and do not correspond to what they pay for. Moreover, internet access in remote areas remains poor; almost all companies concentrate their operations and promotions in the capital, Amman.

The government does not generally block access to digital media. In fact, web 2.0 applications and sites—including global platforms like the social-networking site Facebook, the microblogging service Twitter, and the video-sharing site YouTube—are very popular, particularly among younger Jordanians. The number of Jordanian subscribers to Facebook has surpassed 1.2 million in December 2010, with women accounting for an estimated 42 percent of the total.[9]

The telecommunications and internet sector is bound by Law No. 13 of 1995 and its amendment, Law No. 8 of 2002. The law endorses open-market policies and principles, governs licensing and quality assurance, and prescribes fines and one month to one year in prison for the distribution of improperly obtained content from any internet or telephone communication.[10]

There are currently 11 major internet-service providers (ISPs) in Jordan, though licenses have been granted to over 20 companies. The market is dominated by Omniyah, Zain, and the Jordan Telecom Group, the local affiliate of France Telecom Group's Orange brand. The formerly state-owned Jordan Telecom controls the fixed-line network and provides access to all other ISPs, thereby centralizing the connection to the international internet. Orange Internet, with over 60 percent of all fixed-line broadband subscriptions, is the largest ISP. In March 2010, Orange announced the launch of the country's first third-generation (3G) mobile network, which is expected to contribute to growing internet penetration in the kingdom.

LIMITS ON CONTENT

Jordanian authorities in recent years have appeared uncertain about internet freedom and how best to regulate it. Recurrent threats to filter websites and censor online content have surfaced when political discussions on news websites grow heated, and rarely does a year go by without new legislation or court rulings aimed at the media sector. Even a fellow news

[9] "Jordan—Data for 12/16/2010," Checkfacebook.com, Accessed on February 15, 2011

[10] Arabic Network for Human Rights Information, "Jordan," in *One Social Network With A Rebellious Message* (Cairo: Arabic Network for Human Rights Information, 2009), http://www.openarab.net/en/node/1618.

outlet, the daily newspaper *Al-Ghad*, criticized news websites in 2009 and called on the government to impose more restrictions on online content.

Government officials met with journalists at a 2009 conference of the Jordan Press Association, during a period of legal attacks on news websites. Reaching a reconciliation with the journalists, they pledged to drop pending lawsuits and refrain from issuing legislation to censor online content. However, in January 2010, the Court of Cassation ruled that websites and electronic media must comply with the Press and Publications Law. The ruling raised concerns among media freedom advocates that the content restrictions already imposed on newspapers would be formally extended to online outlets.[11]

Even without specific legislation, website owners often remove material after receiving informal complaints via telephone from government officials, members of the security services**,** party leaders, lawmakers, journalists, and ordinary users. In 2009–10, news websites have had to deal with waves of angry comments from the public whenever sensitive issues are tackled. It is often readers, in addition to state officials, who pressure websites to toe the line and respect traditions.

Outright blocking of websites by the authorities is rare. The only permanently blocked website is the US-based *Arab Times* newspaper, which often takes a critical tone toward Arab regimes and prominent figures in Arab countries.[12] In 2008, the Amman municipality decided to block 600 websites on its internal network, including all Jordanian news websites and newspapers.[13] According to the authorities, this step was taken to prevent municipality employees from wasting time while surfing the net, although several outlets questioned this explanation and suggested that the decision was made due to their critical coverage of the municipal government. Similarly, in August 2010, the state government blocked access to 40 websites from its internal network after a study suggested that public service employees were spending hours surfing websites not related to their work.[14]

Blogs in Jordan, which initially contributed to residents' discovery of the internet as a free source of information, seem to have lost some of their influence. They blossomed at the end of 2005, when bloggers successfully and professionally covered the terrorist attacks on three hotels in Amman. These outlets were quick to respond to the events comprehensively, offering photography and video that traditional media did not provide.[15] Although Jordan's blogosphere flourished for a time after the attacks, it remained marginalized. Online readers

[11] Hani Hazaimeh, "Court Ruling Threatens Press Freedom—Activists," *Jordan Times*, January 15, 2010, http://www.jordantimes.com/?news=23196.
[12] See "Jordan" OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/jordan.
[13] Arab Archives Institute, "Fear of Freedoms: King Insists on Freedoms, Government Resists," news release, December 6, 2008, http://www.ifex.org/jordan/2008/12/09/capsule_report_despite_advances/.
[14] "Public Employees Wasting Time on the Internet," Jordan Times, August 5, 2010, http://www.jordantimes.com/index.php?news=28938.
[15] Arabic Network for Human Rights Information, "Jordan."

tilted more toward political news websites, where they felt they were interacting with a larger audience and receiving more feedback on their comments.

The main blogs are produced by journalists seeking more freedom to post their views without their editors' predictable censorship. They still practice self-censorship and rarely cross the standard red lines, particularly concerning material that could be perceived as harmful to national security, national unity, the country's economy, or the royal family. The blogs' substantial difference from traditional media is the interaction they allow between journalists and their readers. Anonymous comments are permitted on most blogs and readers often take different virtual identities when posting their opinions and complaints. Many blogs are also bilingual and accept feedback in both Arabic and English.

Popular blogs generally tackle human rights, corruption issues, and political developments. Blogs that emphasize the need for free expression include the *Black Iris of Jordan* (http://www.black-iris.com), *What's Up in Jordan?* (http://ajloun.blogspot.com), *360east* (http://www.360east.com), and *7iber* (http://www.7iber.com). Osama Romoh's blog (http://osamaa.com) was named best weblog by Deutsche Welle users in June 2010. The Jordanian blogger writes satirically about social issues and developments in his country. Female bloggers such as Lina Ejeilat, one of the founders of *7iber*, are also making headway and finding more freedom of expression online; for decades, traditional newspapers had reserved the important news coverage and opinion columns for male writers. Social networking tools were also used during the November 2010 elections, and in at least one instance, were important for uncovering allegations of fraud.[16]

VIOLATIONS OF USER RIGHTS

Laws that hinder free expression and access to information include the Jordan Press Association Law (1998), the penal code (1960), the Defense Law (1992), the Contempt of Court Law (1959), the Protection of State Secrets and Classified Documents Law (1971), and the Press and Publications Law (1999). These measures reflect a culture of secrecy that has persisted since the end of martial law in 1989. An Access to Information Law was enacted in 2007, but it contains a number of restrictions. For example, the law bars public requests for information involving religious, racial, ethnic, or gender discrimination (article 10), and allows officials to withhold all types of classified information, a very broad category (Article 13).[17]

The government passed a new cybercrime law in August 2010, despite protests from online activists. The law, which proscribes penalties for cybercrimes such as hacking and

[16] Betsy Fisher, "Jordan: Tweets Cover Parliamentary Elections Flaws," Global Voices, November 10, 2010, http://globalvoicesonline.org/2010/11/10/jordan-tweets-cover-parliamentary-election-flaws/.
[17] Arab Archives Institute, "Summary of the Study on Access to Information Law in Jordan," June 2005, http://www.alarcheef.com/reports/englishFiles/accessToInformation.pdf.

online identity theft, also contains several provisions that could be easily used to suppress free online expression. For example, the new law prohibits posting any information on the web already not available to the public concerning national security, foreign affairs, the national economy, and public safety. It also prohibits publishing any form of "defamation, contempt, or slander," but it does not specify what constitutes each of those crimes. Moreover, the law allows the police to conduct searches and access computers at online media outlets without previously obtaining a warrant from public prosecutors. In protest to the new law, several news sites have expressed interest in registering out of Lebanon.

So far, Jordan's leadership has placed emphasis on reconciliation over severe punishment when dealing with its domestic opponents. Nevertheless, some online commentators have faced legal harassment. Some 20 legal cases were reportedly filed against Jordan-based news websites in 2009.[18] In one instance, Khaled Mahadin, a leading columnist and former adviser to the late king Hussein, was dragged in and out of court for months after criticizing the personal expenses of parliament members. In an article published on the news website Khaberni, Mahadin urged the king to dissolve the parliament because of the "illegal privileges" enjoyed by its members at the expense of Jordanian taxpayers.[19] He was acquitted of defamation in late April, but at the age of 68, exercising freedom of opinion proved costly to his health.

The threat presented by the restrictive laws that remain on the books, combined with an awareness of extensive content monitoring, has a chilling effect on expression online. Bloggers and news website owners often complain directly or indirectly about their inability to post news freely due to monitoring. Jordanians are careful when they talk on mobile phones, and extra prudent about what they say at public meetings. This attitude has passed naturally to the internet, where every word and comment is not only read but documented by date, internet-protocol (IP) address, and location. In a 2010 casee that solidified this suspicion, a Jordanian college student Imad Al-Ash was sentenced to two years in prison after security forces accused him of insulting the king in an instant message to a friend and posting "controversial religious opinions" in public online forums.[20]

Cybercafes, where users might otherwise write with more anonymity, have been bombarded with a series of restrictive regulations and instructions over the past decade. Beginning in the summer of 2010, operators have been obliged to install security cameras to monitor customers, who in turn must supply personal identification information before they use the internet. Cafe owners are required to retain the browsing history of users for at least

[18] Oula Farawati, "Jordan's News Websites Running for Legal Cover," Menassat, March 11, 2009, http://www.menassat.com/?q=ar/comment/reply/6143.
[19] Reporters Without Borders, "Court Acquits Well-Known Columnist of Defaming Parliament," news release, April 29, 2009, http://en.rsf.org/jordan-court-acquits-well-known-columnist-29-04-2009,32743.html.
[20] Ahmad Al-Shagra, "Jordanian Student Sentenced to 2 Years Over IM," *The Next Web*, July 19, 2010, http://thenextweb.com/me/2010/07/19/royal-ash-jordanian-student-sentenced-to-jail-for-2-years-over-im/.

six months.[21] Authorities claim these restrictions are needed for security reasons. In any case, the once-thriving cybercafe business is now in decline due to the restrictions as well as the decrease in the cost of home connections.

In addition to government monitoring, news websites and online writers face intimidation by traditionalist readers, who flood their comments sections with threatening messages in a bid to muzzle independent thought and free expression. Moreover, websites such as Ammonnews.net, Khaberni.com, and Jorday.net have been subjected to hacking attacks whenever sensitive material is posted or during times of social tension.

[21] International Freedom of Expression Exchange, "Cyber crime law attacks free expression; Internet cafés monitored," August 18, 2010, http://www.ifex.org/jordan/2010/08/18/cyber_cafe/

KAZAKHSTAN

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Partly Free**
Obstacles to Access	n/a	16
Limits on Content	n/a	22
Violations of User Rights	n/a	17
Total	**n/a**	**55**

POPULATION: 16.3 million
INTERNET PENETRATION: 28 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Kazakhstan's government has sought to make the internet a new source of economic strength and build the country into the information-technology hub of Central Asia. With that goal in mind, the government has made modest efforts to liberalize the telecommunications sector, promote internet usage, and enhance the internet portals of state entities. At the same time, the authorities also attempt to control citizens' access to information and apparently fear the internet's democratizing potential. In recent years, the government has blocked a popular blog-hosting platform and passed several pieces of legislation that restrict free expression online, particularly on topics that are deemed threatening to President Nursultan Nazarbayev's power and reputation.

Kazakhstan's .kz internet country code was registered in 1994, and its first websites in Russian and Kazakh were launched in 1996 and 1998, respectively. The main ministries and agencies responsible for regulating information and communication technologies (ICTs) were established in 2004 and 2005. A few years later, the government initiated several programs to promote internet use, such as a plan to lower digital inequality and a scheme to expand online government functions. This trend continued in 2010, with the creation of a new Ministry of Communications and Information tasked with formulating an ICT development strategy for 2010–14.[1]

[1] Adil Soz, "Отменена Концепция развития единого информационного пространства казахстанского сегмента сети Интернет на 2008–2012 гг" [Development Concept of the United Information Space of the Kazakh Segment of the Internet for 2008–2012 Is Canceled], Internews Kazakhstan, May 19, 2010, http://www.internews.kz/newsitem/19-05-2010/11551.

OBSTACLES TO ACCESS

Over the past decade, internet access has grown exponentially, from a 0.7 percent penetration rate in 2000 to 28 percent—or 4.3 million users—by the end of 2010, according to official figures.[2] The International Telecommunications Union offers a somewhat lower number, 2.8 million users, as of 2009.[3] Some 92 percent of users access the internet several times per month. In terms of user demography, 44 percent are female, 94 percent are Russian speakers, 4.5 percent are Kazakh speakers, and 1.4 percent are English speakers, with most accessing the internet from urban areas.[4] Because employers increasingly block access to entertainment sites, social-networking applications, and personal e-mail providers with the aim of maintaining worker productivity, most users access the internet from home. Some research studies also show that the number of people using the internet per household is growing, reaching 2.4 in 2010.[5] In recent years, there has also been a shift from dial-up to broadband connections. In 2007, up to 70 percent of connected households used dial-up, but by 2009, some 80 percent had a broadband connection with the state-owned Kazakhtelecom (Megaline), the least expensive provider at approximately US$30 per month.[6] Although cybercafes were popular earlier in the decade, their numbers have dropped significantly in recent years, as users can now connect at home for half the cost of using a cybercafe.[7] Nevertheless, even Kazakhtelecom's broadband rate remains difficult for many people to afford, as the minimum monthly wage is approximately US$90.[8] The cost of internet access for most private subscribers in Kazakhstan is broken into a two-tiered system: access to information hosted inside the country is unlimited, but for content hosted outside Kazakhstan, users are required to pay an additional fee for traffic that exceeds a monthly allowance determined in their contract.

[2] Muratbek Makulbekov, "Kazakhstan has 4.3 mln Internet users—Minister of Communications and Information," KazInform, January 10, 2011, http://www.kazinform.kz/eng/article/2338805.

[3] International Telecommunications Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

[4] OpenNet Initiative, "Country Profile: Kazakhstan," May 10, 2007, http://opennet.net/research/profiles/kazakhstan.

[5] Aleksandr Vasilyev, "Казнет в разрезе" [Kaznet in Section], *Computer Club Magazine*, March 12, 2010, republished by Profit Online at http://www.profit.kz/articles/001192/.

[6] Vasilyev, ""Казнет в разрезе."

[7] Yulia Semykina, "Интернет-кафе Алматы" [Internet Cafe Almaty], *Kontinent,* June 13, 2007, republished by Profit Online at http://www.profit.kz/articles/000205.

[8] Kazakhstan Today, "Прожиточный минимум в Казахстане в октябре составил 13 161 тенге" [Subsistence Minimum in Kazakhstan in October Amounted to 13,161 Tenge], Zakon.kz, November 2, 2009, http://www.zakon.kz/152083-prozhitochnyjj-minimum-v-kazakhstane-v.html; Mojazarplata.kz, "Что такое минимальная заработная плата?" [What Is the Minimum Wage?], http://mojazarplata.kz/main/dohody-minimum/Minimalnaja_zarplata/minimalnaja-zarplata, accessed May 14, 2010.

Some advanced web applications are available and quite popular; in mid-2010, the fifth-most-visited website in Kazakhstan was the Russian social-networking platform Vkontakte.ru.[9] The video-sharing website YouTube and the microblogging service Twitter are also growing in popularity. However, the international blog-hosting platform LiveJournal was blocked beginning in October 2008 by the two largest internet-service providers (ISPs), the state-owned Kazakhtelecom, and Nursat, though the companies refused to acknowledge the filtering.[10] The impetus for the block was to restrict access to content posted by Rakhat Aliyev, Nazarbayev's former son-in-law (see "Limits on Content"). In November 2010, shortly before Kazakhstan hosted a summit of the Organization for Security and Co-operation in Europe (OSCE), LiveJournal administrators froze Aliyev's account, possibly due to pressure from the Kazakh authorities. The platform was subsequently unblocked after over two years of being inaccessible.[11] Access to Blogger.com was similarly restricted, with the exception of sporadic openings, for much of 2010.[12]

With nearly 15 million users, mobile-phone penetration reached approximately 95 percent by 2009, and has continued to grow since.[13] The number of users accessing the internet via mobile devices is also increasing, though the mobile internet penetration rate was only 7 percent in 2010.[14] While mobile internet access is relatively new to the market, its advertising revenue is on the rise. During the last three years, WiMax networks have also become available in Kazakhstan.

The state-owned Kazakhtelecom is the largest ISP and holds a 48 percent market share.[15] Another six operators are licensed to connect to the international internet. However, they are required to channel at least part of their traffic through Kazakhtelecom's infrastructure.[16] Over 100 other ISPs operate in Kazakhstan, but must purchase their access via the above-mentioned seven, making it difficult for them to compete in the market. As such, the five largest companies account for some 90 percent of the internet access market. Kazakhtelecom's dominance over information flow routes creates the conditions for systemic content filtering and surveillance. As of mid-2010, there were six mobile-phone

[9] Alexa, "Top Sites in Kazakhstan," http://www.alexa.com/topsites/countries/KZ, accessed August 25, 2010.
[10] Karin Deutsch Karlekar, eds., "Kazakhstan," *Freedom of the Press 2009* (New York: Freedom House, 2008), http://www.freedomhouse.org/template.cfm?page=251&year=2009.
[11] Adil Nurmakov, "Kazakhstan: Livejournal Unblocked After 2 Years of Filtering," Global Voices Online, November 17, 2010, http://globalvoicesonline.org/2010/11/17/kazakhstan-livejournal-unblocked-after-2-years-of-filtering/.
[12] Google, "Transparency Report: Traffic," http://www.google.com/transparencyreport/traffic/, accessed September 23, 2010.
[13] International Telecommunications Union, "ICT Statistics 2009–Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/CellularSubscribersPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False, accessed September 23, 2010.
[14] Vasilyev, "Казнет в разрезе."
[15] Inna Soboleva, "Рынок телекоммуникаций: динамика развития" [Telecommunications Market: Dynamics of Development], *Advertising*, September 30, 2006, republished by Profit Online at http://www.profit.kz/articles/000126/.
[16] OpenNet Initiative, "Country Profile: Kazakhstan," *Access Controlled*, http://www.access-controlled.net/wp-content/PDFs/part2/007_Kazakhstan.pdf, accessed September 23, 2010.

providers in Kazakhstan, including three using the GSM standard and three using the CDMA standard. The three most active are GSM Kazakhstan, Beeline/K-Mobile, and Altel.[17] Kazakhtelecom holds a stake of 49 percent in GSM Kazakhstan, and is also a parent company to one of the other GSM carriers, NEO.[18] Beeline belongs to the Russian mobile operator Vimpelcom, which acquired the Kartel company and its K-Mobile system in 2005.[19]

Several bodies regulate the ICT sector. The .kz domain is managed by the Kazakh Center of Network Information and the Kazakh Association of IT Companies; both were created in 2004–05. The latter was established as a nongovernmental organization, but in practice, it reportedly has 80 percent government ownership, and has been known to make politicized decisions on the registration .kz domain names.[20] Among government entities, ICT issues have been overseen mostly by the Informatics and Communications Agency and the Ministry of Culture, which were restructured in 2010 and merged into the Ministry of Communications and Information.

The government-affiliated Kazkontent organization is responsible for creating strategies and programs to help the Kazakh internet generate more of its own content. Since 2009, ISPs have also collaborated within the National Center for Internet Traffic Exchange to set up special channels for routing traffic during high-demand periods. As of mid-2010, eight ISPs were participating in the network, including four of the largest operators: Kazakhtelecom, Nursat, Intelsoft, and Astel.

LIMITS ON CONTENT

The Kazakh authorities have engaged in some online censorship, though it is selective, sporadic, and inconsistent. Nevertheless, there are indications that government censorship may expand in the coming years, including possibly via filtering at the backbone network level.[21] In addition, in March 2010, Kuanyshbek Yesekeyev, who heads the Kazakh Information and Communication Agency, announced the establishment of the "Service to React to Computer Incidents." He stated that it had begun compiling blacklists of

[17] Valentina Fomicheva, "Мобильная связь в Казахстане" [Mobile Communications in Kazakhstan], *Computer Club Magazine*, March 26, 2007, republished by Profit Online at http://www.profit.kz/articles/000162/.
[18] "KazakhTelecom to Sell Mobile Network Subsidiary," Cellular News, June 29, 2009, http://www.cellular-news.com/story/38266.php.
[19] "Kartel (K-Mobile) GSM Network Expansion, Kazakhstan," Mobilecomms Technology, http://www.mobilecomms-technology.com/projects/kartel/, accessed February 15, 2011.
[20] OpenNet Initiative, "Country Profile: Kazakhstan."
[21] OpenNet Initiave, "Country Profile: Kazakhstan."

"destructive" websites, raising concerns among free expression advocates that such a vague criterion would be applied to politically and socially-oriented websites.[22]

There are three ways in which access to certain online content is restricted in Kazakhstan: technical filtering by Kazakhtelecom, cancellation of .kz domain names, and more recently, self-censorship by content hosting companies for fear of prosecution.

According to testing conducted by the Open Net Initiative (ONI) on two principle ISPs, access is blocked—particularly by Kazakhtelecom—to "opposition groups' websites, regional media sites that carry political content,…selected social networking sites, [and] a number of proxy sites."[23] Censorship is often inconsistent, however, and in some cases blocks are only implemented by Kazakhtelecom. Service providers that use their own channels to connect to the wider internet may provide access without blocking. During its two-year blockage, LiveJournal, for example, could be accessed freely in several cybercafes in Almaty that did not connect via Kazakhtelecom. Similarly, in some instances, websites that are blocked on the regular internet appear to be accessible via mobile devices. Throughout 2010, the main website of *Respublika,* an opposition weekly paper known for its criticism of the government and coverage of sensitive topics such as human rights abuses and high-level corruption, was blocked for most Kazakh users, corresponding to increased official repression targeting its print edition. A reader survey conducted by the editors revealed that Kazakhtelecom customers were unable to access the site, but readers served by other ISPs were able to load it.[24] Both the government and Kazakhtelecom executives have avoided commenting on censorship policies, preferring to remain silent or attribute content inaccessibility to technical problems.

One of most visible catalysts for censorship has been the political scandal surrounding Rakhat Aliyev, Nazarbayev's former son-in-law, who had served as chair of the National Security Committee for Almaty, and as ambassador to Austria before definitively falling out of favor with the president and his family. He was then sought by the authorities on charges of kidnapping and financial crimes. Having fled abroad, he began airing inside information and allegations, in the traditional media and online, in an effort to discredit the president. Any material related to Aliyev and his connections to the presidential family is filtered by Kazakhtelecom. In October 2007, four opposition-related websites (Kub.kz, Zonakz.net, Geo.kz, and Inkar.info) were blocked after they had posted transcripts of phone conversations among high-level politicians related to the Aliyev case.[25]

[22] "Kazakhstan Tightens Control Over Internet—Official," Inquirer.net, March 1, 2010, http://newsinfo.inquirer.net/breakingnews/infotech/view/20100301-256094/Kazakhstan-tightens-control-over-Internetofficial ; Nina Ognianova, "Disdaining Press Freedom, Kazakhstan Undermines OSCE," Committee to Protect Journalists, September 14, 2010, http://cpj.org/reports/2010/09/disdaining-press-freedom-kazakhstan-undermines-osc.php.

[23] OpenNet Initiative, "Country Profile: Kazakhstan."

[24] Ognianova, "Disdaining Press Freedom, Kazakhstan Undermines OSCE."

[25] Bruce Pannier, "Kazakhstan Blocks Critical Websites, as Opposition Cries 'Censorship'," *Radio Free Europe, Radio Liberty*, October 24, 2007, http://www.rferl.org/content/article/1079017.html.

While Zonakz.net and Inkar.info were soon unblocked, access to Kub.kz and Geo.kz was permanently restricted when the authorities withdrew their registration for a .kz domain name. In late October 2007, the Kazakh Agency for Information and Communication issued an order to shut down the websites, citing 2005 rules requiring all .kz sites to be hosted in Kazakhstan, while these two websites were based overseas.[26] A similar justification was used to suspend Borat.kz in 2005 after a wave of resentment among Kazakh authorities against the American film *Borat*, which parodied the country.[27]

With several new pieces of internet-restricting legislation coming into force, since early 2009 there has also been an increase in self-censorship and content removal implemented by companies hosting online information.[28] Despite criticism from the international community, in July 2009 Nazarbayev signed amendments to the existing information and communication law that identified all online resources—including websites, chat rooms, blogs, online stores, and electronic libraries—as mass media with equal civil, administrative, and criminal responsibility. The law also calls for the blocking of any online resources that carry elements of "information war against Kazakhstan," whether or not the server and domain hosting the information is located in the country.[29] Given the harsh legal environment for traditional media, the legislation opened the door for "third-party liability," in which the owner or host of a website is held legally responsible for content posted by others, for instance in discussion forums or the comment section under a news article. Following passage of the amendment, most online content providers in Kazakhstan hired moderators to monitor and censor content that could expose the hosting entity to legal repercussions. It is impossible to create any account with the name Rakhat Aliyev, for example. Many observers warn that such self-censorship will grow worse due to the July 2010 adoption of a law granting Nazarbayev the status of "Leader of the Nation," which essentially places any criticism of him and his family under the umbrella of threats to "national" security or reputation. However, the threat of third-party liability has not yet influenced foreign search engines such as Russia's Yandex or the U.S.-based Google, which do not censor their search results.

The 2008 blocking of LiveJournal, at the time the most popular blogging platform in Kazakhstan, generated significant changes to the country's blogosphere. Before it was blocked, LiveJournal hosted 32 percent of all active Russian-language blogs in Kazakhstan,

[26] A copy of the letter from the Kazakh Center of Network Information to Kub.kz informing it of its suspension is available at http://www.kub.info/downloads/kaznic.pdf, accessed August 30, 2010.
[27] "Kazakhs Shut Ali G Star's Website," British Broadcasting Corporation, December 14, 2005, http://news.bbc.co.uk/2/hi/entertainment/4527516.stm.
[28] Carl Schreck, "Kazakhstan Puts Pressure on Bloggers," The National, August 25, 2009, http://www.thenational.ae/apps/pbcs.dll/article?AID=/20090825/FOREIGN/708249847/1140.
[29] The text of the law is available in Russian at http://comport.region.kz/forum/download/file.php?id=7262, accessed August 30, 2010.

or nearly 230,000 users,[30] and there were no local platforms. Some bloggers migrated to other international platforms like Blogger.com or LiveInternet.ru, while others retained their blogs on LiveJournal but used a proxy server to access it. Still others switched to new local services supported by Kazakhtelecom. As of the end of 2010, it was too soon to tell if these shifts would be reversed with LiveJournal's unblocking.

One of the local blogging sites, Yvision.kz, has emerged as the most popular Kazakhstan-based blog-hosting platform, with over 14,000 users blogging mostly in Russian. Many of the platform's creators are bloggers and programmers, but they have had to introduce a system to moderate and self-censor content, and anyone joining the site must accept a user agreement outlining the system. Yvisioners coined the term "yvizhenka," referring to a series of "offline" meetings of bloggers that have been held periodically in almost every large city in Kazakhstan since 2009. Noticing the emerging market for blog-hosting platforms, another large-scale blogging project called On.kz was launched in 2010. According to the project's managers, more than 15,000 blogs were registered during the first few months. Overall, however, the Kazakh blogosphere remains a relatively small community with room to grow.

In an effort to counter criticism of the blocking of LiveJournal and demonstrate a willingness to engage with citizens online, government officials started to keep their own blogs in recent years. Every government website has a blog, and according to the prime minister, every minister should establish a blog and write about the work being done by their ministry. The website blogs.egov.kz is called "the official blogging platform for high-ranking Kazakh officials," and is home to the blog of Prime Minister Karim Masimov, among others.[31] The initiative appears to have attracted little attention and had a limited impact on public opinion as the blogs generally resemble other government press portals in style and content.

The Kazakh blogosphere is dominated by the younger generation, with most users aged between 15 and 25.[32] Although blogs typically focus on personal topics, entertainment, and fashion, blogging has become a popular tool for self-promotion. As same-sex relationships are not widely accepted in the country, people writing on the issue often prefer to keep their blogs in "friends-only" mode, fearing societal discrimination should their sexual orientation become publicly known. Nevertheless, in July 2010, the first gay and lesbian literary magazine was published and made available online, as many of the

[30] Human Rights Watch, "Human Rights in Kazakhstan: Seven Months Before the OSCE Chairmanship," memorandum, May 20, 2009, http://www.hrw.org/node/83329.

[31] Adil Nurmakov, "Kazakhstan: Prime Minister Launched Blog," Global Voices, January 16, 2009, http://globalvoicesonline.org/2009/01/16/kazakhstan-prime-minister-launched-blog/.

[32] Anna Shaternikova, "Недостаточно высокий уровень проникновения Интернета и выбор пользователями российских ресурсов препятствуют развитию казахстанского контента и распространению коммерческих интернет-услуг" [Insufficiently High Level of Internet Penetration and User Choice of Russian Resources Hinder the Development of Kazakhstan's Content and Distribution of Commercial Internet Services], *Panorama*, May 8, 2010, republished by Zakon.kz at http://www.zakon.kz/171765-nedostatochno-vysokijj-uroven.html.

contributors were bloggers. In terms of blocked content, particularly related to Aliyev, many users are not politically active or interested in accessing his writings. Those who wish to, may access them fairly easily via proxy servers and relatively simple channels like Google translate or Opera's Turbo browser. The authorities have not engaged in significant efforts to stop such circumvention.

Civic activism aimed at promoting internet freedom is rare, though there are a few well-known nongovernmental organizations working on the topic. For example, Adilsoz, Internews, and Medianet execute monitoring projects, and report on violations of free expression or recent trends on the Kazakh internet. One recent initiative, the "For a Free Internet" campaign, started as a journalists' protest against the closure of the newspaper *Respublika*, but evolved into a movement for internet freedom. Supporters carried out a few "flash mobs," sudden protests that were planned online, in May 2009 and April 2010, to oppose changes to internet legislation, though there were no clear reports on the number of participants. The campaign has also monitored the blocking of websites and filed more than 120 lawsuits to challenge decisions to block certain websites; three of the cases have moved forward.[33] Overall, civil society activists and the blogging community lack coordination and an understanding of one another's needs, leading to limited political activism in Kazakhstan in comparison with neighboring countries like Kyrgyzstan."

VIOLATIONS OF USER RIGHTS

The Kazakh constitution guarantees freedom of the press, but also provides special protection for the president, and in practice, the authorities use various tactics to control the media and limit free expression. Since 2008, the Kazakh government has taken steps to significantly change the legal landscape governing the media. First, under pressure from the Organization for Security and Cooperation in Europe (OSCE), amendments aimed at liberalizing media legislation were adopted in February 2009. The changes simplified the registration process for electronic media, made it possible for the media to challenge official denials of access to information in court, and allowed media workers to use audio recorders and cameras to collect information without asking for the permission of those recorded.[34] Although the amendments reduced some bureaucratic obstacles, they did little to contribute to political liberalization. Instead, separate draft amendments were submitted to impose new restrictions on the internet and other media entities via changes to the media law, the law on national security, the civil procedure code, the administrative code, and other laws.

[33] Law and Mass Media of Central Asia, "Более 120 интернет-пользователей подали иски в адрес Министерства связи и информации" [More Than 120 Internet Users File Lawsuits Against the Ministry of Communication and Information], news release, May 21, 2010, http://www.medialawca.org/node/5647.
[34] Human Rights Watch, "Human Rights in Kazakhstan."

By the summer of 2009, these amendments were all adopted, despite protests from civil society and the international community.

The amendments declared the internet and content on all websites worldwide to be "internet resources," without differentiating between news sites, private blogs, and chat rooms. According to the law, the prosecutor general has the power to suspend any mass media outlet, including any website, "in cases where the violation is clear" and "could pose significant harm to the protected legal interests of the public and the state," and when a "quick intervention is needed to protect the interest of state and society."[35] Publications involving classified information, extremist propaganda, and pornography can also be restricted.

One year after the parliament adopted these changes, it passed the law granting the current president the status of "Leader of the Nation." According to the law, Nazarbayev will have the power to decide on questions related to the state even after he leaves the presidency, and will be granted immunity for any actions taken while he was in office. In addition, any infringement on his life is considered terrorism, and criminal responsibility is attached to any damage done to his image, including public insults or distortion of his private biographical facts.[36] Thus, after two years of blocking websites and censoring information connected to the Aliyev case, the Kazakh authorities now have a legal justification for restricting access to such information, no longer needing to rely on references to "technical problems."

Although cases of imprisonment of journalists or human rights defenders, as well as closures of media outlets, have increased in the past two years, no bloggers have been prosecuted during this time. In April 2010, however, two activists—Zhanna Baytelova and Irina Mednikova—were arrested while protesting in front of Kazakhtelecom against the blocking of LiveJournal and Respublika's websites; Baytelova was fined $US 190, and Mednikova was given an official warning for organizing an "unsanctioned public gathering."[37]

It is difficult to track or verify efforts by the National Security Committee (KNB) to monitor the internet and mobile-phone communications. However, a series of regulations approved in 2004 obliges ISPs to retain records of users' online activities, including via installation of special software and hardware. The information stored reportedly includes log-in times, session duration, user IP address, and speed of transmission.[38] Systematic monitoring is also suggested by the speed with which content deemed threatening to the regime has been removed or blocked. In June 2010, shortly before the "For a Free Internet"

[35] Human Rights Watch, "Human Rights in Kazakhstan."

[36] "Закон о лидере нации вступил в силу" [Law on the Leader of the Nation Comes Into Force], Today.kz, June 15, 2010, http://www.today.kz/ru/news/kazakhstan/2010-06-15/leader1.

[37] "Kazakh Activists Fined for Protesting Website Ban," *Radio Free Europe, Radio Liberty,* April 24, 2010, http://www.rferl.org/content/Kazakh_Activists_Fined_For_Protesting_Website_Ban/2023347.html.

[38] OpenNet Initiave, "Country Profile: Kazakhstan."

movement planned to hold a protest event involving the drifting of paper boats on asphalt,[39] one of the organizers, civil society activist Dmitry Shelokov, was summoned by the KNB. He refused to come, as there was no written notice, and the activity continued as planned. Following the event, Shelokov received a written notice from the agency. Although several journalists and political activists have allegedly been beaten or received threatening phone calls from the KNB,[40] there have been no reports of bloggers suffering such extralegal harassment.

Several of the opposition-related websites such as *Respublika* that have been sporadically blocked have, according to their administrators, also suffered denial-of-service attacks, the first of which occurred in February 2009.[41] However, the nature and origin of the attacks have not been independently confirmed or investigated by the police.

[39] Askar Shaygumarov, "За бумажные кораблики—в КНБ" [For Paper Boats—To KNB], *Respublika*, June 2, 2010, http://www.respublika-kaz.info/news/politics/9302/.

[40] Dilbegim Mavlony, "Перечень угроз пополнился попыткой вербовки и подворным обходом журналистов" [List of Threats Against Journalists Grows with Recruiting Attempts and Home Visits], Radio Azattyk, September 30, 2009, http://rus.azattyq.org/content/Natalia_Panova_Ekaterina_Belaeva_/1840192.html.

[41] "Интернет-СМИ «Фергана.Ру», Zona.kz и «Республика» были атакованы неизвестными хакерами почти одновременно" [Internet Media 'Fergana.ru,' Zona.kz and 'Respublika' Are Attacked by Unknown Hackers Almost Simultaneously], Fergana.ru, February, 20, 2009, http://www.ferghana.ru/news.php?id=11348.

KENYA

	2009	2011
INTERNET FREEDOM STATUS	Partly Free	Partly Free
Obstacles to Access	13	12
Limits on Content	11	9
Violations of User Rights	10	11
Total	34	32

POPULATION: 40.1 million
INTERNET PENETRATION: 10 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Use of the internet and mobile telephones is relatively unfettered in Kenya, and access to the technology continues to grow. Although a lack of infrastructure and high costs still hamper connectivity for many Kenyans, the installation of two undersea cables in 2009 has dramatically improved bandwidth, and prices are starting to come down. Since 2008, there have been no confirmed incidents of government filtering or interference with online communication. However, in January 2009, the government passed a controversial Communications Amendment Act despite warnings from civil society groups that it could hinder free expression.

The internet was first made available in Kenya in 1993, and the first commercial internet-service provider (ISP) began operating in 1995.[1] Mobile phones were introduced in 1992, but only became widely available and affordable after the Communications Commission of Kenya (CCK) was established and two service providers—Safaricom and Kencell—were licensed in 1999.[2]

[1] Francisca Mweu, "Overview of the Internet in Kenya," International Telecommunication Union (prepared for African Internet & Telecom Summit, Banjul, The Gambia, June 5–9, 2000), http://www.itu.int/africainternet2000/countryreports/ken_e.htm.
[2] Export Processing Zones Authority, *Kenya's Information & Communications Technology Sector 2005* (Nairobi: Export Processing Zones Authority, 2005), http://www.epzakenya.com/UserFiles/File/ictKenya.pdf.

OBSTACLES TO ACCESS

Internet penetration in Kenya has continued to rise gradually, from 7.9 percent in 2008 to nearly 10 percent, or about four million users, in 2009, according to the International Telecommunication Union and the CCK.[3] This trend is expected to continue in the coming years due to increased internet access through mobile phones and improved bandwidth via undersea cables.[4] In 2009, the installation of cables known as Seacom and The East African Marine System (TEAMS) increased connection speeds to 13 times the total bandwidth available during the previous year,[5] and raised hopes of greater connectivity in the future. However, costs for the average user did not drop dramatically, as providers claimed that they needed to recoup the cost of investment in the infrastructure before reducing prices.[6]

The mobile-phone penetration rate was estimated at 60 percent as of mid-2010, significantly higher than internet penetration. An additional 28 percent of Kenyans have access to another person's mobile phone, indicating even broader usage.[7] According to the CCK's latest statistics, 1.98 million Kenyans, or 4.75 percent of the population, have accessed the internet via their mobile phones.[8] This group forms the vast majority of users with their own internet subscriptions, as opposed to those who access the internet at cybercafes or other public access points.[9] A recent study by Opera, a software company that monitors trends in mobile browsing, showed that Kenya has the most intensive mobile-internet user community in Africa, with each user browsing an average of 525 pages per month.[10]

Despite these advances, the spread of the internet is hampered by a poor telecommunications infrastructure and lack of electricity, particularly in rural areas. This partly explains the disproportionately high concentration of internet subscribers in Kenya's two largest cities, Nairobi and Mombasa. The government is currently working to remedy the disparity between rural and urban access through the introduction of Pasha digital

[3] International Telecommunication Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx, accessed February 11, 2011; Communications Commission of Kenya (CCK), "Quarterly Sector Statistics Report, Second Quarter Oct-Dec 2009/2010," http://www.cck.go.ke/resc/statistics/Sector_Statistics_Report_Q2_2009-2010.pdf, accessed August 23, 2010

[4] Ian Mansfield, "3G Services and MNP to Drive Kenyan Telecom Sector," *cellular-news*, May 31, 2010, http://www.cellular-news.com/story/43566.php.

[5] CCK, "Quarterly Sector Statistics Report, Second Quarter Oct-Dec 2009/2010."

[6] Catherine Riungu, "No Hope of Cheap Internet with Providers Locked into 25-yr Deals," *East African*, October 5, 2009, http://www.theeastafrican.co.ke/news/-/2558/667644/-/qy9vnkz/-/index.html.

[7] Gunnar Camner, Caroline Pulver, and Emil Sjoblom, *What Makes a Successful Mobile Money Implementation? M-Pesa in Kenya and Tanzania* (Nairobi: Financial Sector Deepening Kenya, 2009), http://www.fsdkenya.org/pdf_documents/09-08-28_MPESA_in_Kenya_Tanzania.pdf.

[8] CCK, "Quarterly Sector Statistics Report, Second Quarter Oct-Dec 2009/2010."

[9] CCK, "Quarterly Sector Statistics Report, Second Quarter Oct-Dec 2009/2010."

[10] Victor Juma, "Mobile Internet on Course to Becoming Top Earner for Firms," *Business Daily*, April 22, 2010, available at http://allafrica.com/stories/201004210995.html.

villages—small public access sites similar to cybercafes.[11] The facilities are estimated to have increased rural usage from 4 percent to 9 percent between 2007 and 2009.[12]

There have been no reports of the government using control over internet infrastructure to limit connectivity. Kenyans have unrestricted access to the social-networking site Facebook, the YouTube video-sharing site, and the blog-hosting site Blogger, all of which rank among the 10 most popular sites in the country.[13]

Reform of Kenya's information and communications sector in 2008 led to a new licensing framework—part of a regulatory strategy that has seen a shift from licensing based on a bidding process to open, market-based licensing.[14] Competition has been introduced in most segments of the telecommunications market, though Safaricom currently dominates mobile-phone services, holding nearly 80 percent of the market.[15] In May 2010, the CCK published the Kenya Information and Communications (Fair Competition and Equality of Treatment) Regulations of 2010, whose objective was to reduce the gap between Safaricom and its competitors. However, in June 2010 the CCK reportedly withdrew the regulations following strident complaints from Safaricom.[16] In addition, the third-generation (3G) mobile service licensing model remains controversial, as only one of the four mobile operators, Safaricom, was able to hold a 3G license until recently. Later in June 2010, the CCK announced that it would be lowering the upfront fees for a 3G license. Safaricom protested, arguing that since it had paid the full KSh 1.9 billion (US$23.4 million) for its license, it should receive compensation from the government if other providers are allowed to pay less.[17] Nevertheless, Zain that month became the second Kenyan operator to receive a 3G license.[18] Another company, Telkom (Orange), obtained a license in November 2010 to launch its own 3G service in the first part of 2011.[19]

Under the Communications Amendment Act, passed in January 2009, the CCK rather than the independent and professional Media Council of Kenya is responsible for

[11] "Kenya Investing Ksh 16.3 Billion in Rural ICT," *Information Policy* (blog), July 30, 2009, http://www.i-policy.org/2009/07/kenya-investing-ksh163-billion-in-rural-ict.html.
[12] Russell Southwood, "Internet Is Creeping Up on Television for Key 18–24 Demographic, Says New National Survey," Balancing Act, February 4, 2010, available at http://allafrica.com/stories/201002050912.html.
[13] Alexa, "Top Sites in Kenya," http://www.alexa.com/topsites/countries/KE, accessed August 23, 2010.
[14] "CCK Heeds Call, Slashes 3G Upfront Fees," KenTV, http://www.kentv.net/news-archive/2511-cck-heeds-callslashes-3g-upfront-fees, accessed February 11, 2011.
[15] Macharia Kamau, "Safaricom Raises Concerns Over Competition Rules," *Standard*, May 3, 2010, http://www.standardmedia.co.ke/InsidePage.php?id=2000008960&cid=14.
[16] Kui Kinyanjui and Mark Okuttah, "Firm Picked to Guide Telcos Regulation," *Business Daily*, June 8 2010, http://www.businessdailyafrica.com/Company%20Industry/Firm%20picked%20to%20guide%20telcos%20regulation/-/539550/933998/-/60qhtd/-/index.html.
[17] Evelyne Njoroge, "Zain Kenya Happy with Move on 3G Licenses," Capital Business, June 18, 2010, http://www.capitalfm.co.ke/business/Kenyabusiness/Zain-Kenya-happy-with-move-on-3G-licenses-4320.html.
[18] Michael Karanja, "Another Kenyan Firm Gets 3G License," Capital Business, June 25, 2010, http://www.capitalfm.co.ke/business/Kenyabusiness/Another-Kenyan-firm-gets-3G-license-4348.html.
[19] Duncan Miriri, "Telkom Kenya Gets Shareholder Loan for 3G License," Reuters, June 23, 2010, http://af.reuters.com/article/investingNews/idAFJOE65M0EU20100623. George Mwangi, "Telkom Kenya Gets 3G License," *Wall Street Journal,* November 24, 2010, http://online.wsj.com/article/BT-CO-20101124-707873.html.

regulating both traditional and online media. The formal independence of the CCK is enshrined in the 1998 Kenya Communications Act, and in 2005 several independent commissioners, including a civil society representative, joined the CCK board. However, most of the commissioners remain government appointees, and their independence is somewhat limited in practice.[20] The CCK's recent withdrawal of the proposed fair competition regulations has reinforced the perception that the commission is subject to the undue influence of powerful companies like Safaricom.[21] As the CCK has yet to make any decisions affecting the internet, its autonomy and professionalism in making determinations on the topic remain to be seen. Access providers have formed organizations such as the Kenyan ISP Association, the Telecommunications Service Providers of Kenya, and the Kenya Cybercafe Owners to lobby the government for better regulations, lower costs, and increased efforts to improve computer literacy.

LIMITS ON CONTENT

The government does not employ technical filtering or any administrative censorship system to restrict access to political or other content. Citizens are able to access a wide range of viewpoints, with the websites of the British Broadcasting Corporation (BBC), the U.S.-based Cable News Network (CNN), and Kenya's *Daily Nation* newspaper being the most commonly accessed online news outlets.[22] Despite concerns over the use of the internet to propagate hate speech during postelection violence in late 2007 and early 2008, and fears that the authorities might use this to justify imposing greater controls on online content, no such restrictions have been introduced. Individual internet users generally seem comfortable expressing themselves freely online, though mainstream media organizations practice some self-censorship.

The internet has emerged as an increasingly important forum for political debate, particularly during the run-up to an August 2010 referendum in which voters approved a new constitution. Political and civic organizations used the internet to distribute educational material such as pamphlets, videos, and statements about their positions on the draft constitution, as well as to publicize rallies related to the referendum. However, as in the run-up to the 2007 elections, there were also concerns that the internet was being used by nonstate actors for detrimental purposes. Some of those opposed to the draft constitution, for instance, spread misinformation about controversial aspects of the document, such as claims that it would legalize abortion. (In fact it contained a clause similar to one in the

[20] Rebecca Wanjiku, "Kenya Communications Amendment Act 2009: Progressive or Retrogressive?" Association for Progressive Communications, September 2009, http://www.apc.org/en/system/files/CICEWAKenya20090908_EN.pdf.
[21] Jevans Nyabiage, "Kenya: Storm Brews Over New CCK Telecoms Rules," *Daily Nation*, May 3, 2010, available at http://allafrica.com/stories/201005031247.html.
[22] Juma, "Mobile Internet on Course to Becoming Top Earner for Firms."

current penal code that allows a doctor to conduct an abortion when the mother's life is in danger.) Aside from the constitutional referendum, the blogging community in recent years has mostly focused on apolitical topics such as the booming technology sector in Nairobi. Meanwhile, print outlets, television, and radio continue to be the main sources of news and information for most Kenyans, though there are increasing efforts to extend mainstream news to online platforms. All major television stations use YouTube to rebroadcast news clips and also have accounts on Facebook and the Twitter microblogging site.

VIOLATIONS OF USER RIGHTS

The constitution protects freedom of expression and the "freedom to communicate ideas and information." However, it also grants the government the authority to punish defamation, protect privileged information, and restrict state employees' freedom of expression "in the interest of defense, public safety, public order, public morality or public health." Criminal defamation laws remain on the books, but there do not appear to have been any cases aimed at online commentators. In January 2009, the president approved the controversial Communications Amendment Act despite significant opposition from local media workers and international press freedom watchdogs. The act established that any person who publishes, transmits, or causes to be published in electronic form obscene information commits an offense. It also outlines other forms of illegality associated with the use of information and communication technologies (ICTs).[23] The prescribed punishments include up to KSh 200,000 (US$2,460) in fines and two years' imprisonment. In July 2009, an amendment to the legislation repealed provisions that had restricted broadcast media. The law's effects on online communications remain unclear,[24] and as of the end of 2010, the measure had not been used to prosecute anyone for online expression.

Surveillance of internet and mobile phones is not a serious concern in Kenya. In June 2010, the CCK announced a requirement for all mobile-phone subscribers to register their SIM cards with their service providers. By September, approximately 60 percent of users had registered and the authorities extended the deadline to allow the remainder time to do so before having their lines disconnected.[25] There have been no reported cases of bloggers or other activists having their communications monitored. There were no reports of extralegal intimidation of journalists, bloggers, or other ICT users by state authorities or any other actor in 2009–10.

[23] Republic of Kenya Office of Public Communications, "The Kenya Communications (Amendment) Act 2009," http://www.communication.go.ke/Documents/media.pdf, accessed February 15, 2011.
[24] International Freedom of Expression eXchange (IFEX), "Triumph for Journalists as Government Agrees to Amend Media Law," news release, May 20, 2009, http://www.ifex.org/kenya/2009/05/20/govt_to_amend_law/.
[25] CCK, "It's now mandatory to register your SIM card," June 21, 2010, http://www.cck.go.ke/news/2010/news_21june2010.html; Simon Davies, "Kenya Extends SIM Card Registration Deadline," Cellular News, September 22, 2010, http://www.cellular-news.com/story/45530.php.

MALAYSIA

	2009	2011
INTERNET FREEDOM STATUS	Partly Free	Partly Free
Obstacles to Access	9	9
Limits on Content	12	11
Violations of User Rights	20	21
Total	41	41

POPULATION: 28.9 million
INTERNET PENETRATION: 56 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

The Malaysian government has actively encouraged access to the internet and mobile phones, and the use of such media has risen rapidly since the first internet-service provider (ISP) was inaugurated in 1992. By the end of 2009, more than half of the population accessed the internet and the figure continues to grow.[1] In the watershed general elections of March 2008, the ruling National Front (BN) coalition lost its two-thirds parliamentary majority for the first time since 1969. In addition, opposition parties won control of five of the 13 states, including those with relatively high internet penetration rates, such as Penang and Selangor. Together with the growing popularity and importance of independent online news outlets, the use of the internet for political mobilization was widely perceived as contributing to the opposition's electoral gains.[2]

In both the run-up to and aftermath of the elections, many observers sensed that the government and ruling coalition had recognized the potential political impact of the internet and had therefore grown more determined to control it. In recent years there has been a series of incidents in which bloggers have been harassed or charged under vaguely worded security laws. The government has also made a more concerted effort to influence public opinion by establishing its own presence online, while several online news outlets and opposition-related websites have faced cyberattacks. However, more systemic forms of

[1] International Telecommunications Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.
[2] "Malaysia's Uneasy Dance with the Web," *Asia Sentinel*, August 17, 2010, http://asiasentinel.com/index.php?option=com_content&task=view&id=2645&Itemid=178.

censorship, such as technical filtering, have not been implemented. Meanwhile, a growing number of Malaysians have begun to blog or to communicate via advanced web applications such as the Facebook social-networking site, the Twitter microblogging service, and the video-sharing site YouTube.

OBSTACLES TO ACCESS

Internet penetration has grown dramatically over the past decade, from 3.7 million users in 2000 to as much as 16.1 million in 2010, according to estimates by the Economist Intelligence Unit.[3] Moreover, according to the Nielson Media Index, almost 4 in 10 users spent one to two hours on the internet every day in 2008.[4] Malaysians can access the internet through home connections, mobile phones, or cybercafes. Cybercafes play an important role in bridging the urban-rural connectivity gap. Nevertheless, there remains an acute digital divide in the country, with more than 80 percent of internet users living in urban areas,[5] and significantly lower penetration rates in the more sparsely populated states of East Malaysia, where most residents belong to indigenous groups.

Mobile-phone use has also increased significantly in recent years. By the end of 2010, the number of subscribers—33.1 million—exceeded the country's total population, meaning some individuals had multiple phone lines.[6] By comparison, mobile-phone penetration was just 21.8 percent in 2000.[7] Given the high overall penetration rate, there is less of an urban-rural divide in mobile-phone use than in internet connectivity.[8] With four active third-generation (3G) service providers, access to 3G mobile technology is expanding, and the number of subscribers reached 8.6 million by the end of 2010.[9] Faster broadband access and the increasing availability of 3G service have allowed a growing number of Malaysian citizens to circulate information via advanced web applications like the video-sharing website YouTube, the social-networking site Facebook, and the microblogging application Twitter. All such applications are freely accessible. In August 2010, however, a politician from the ruling coalition voiced calls for Facebook to be blocked after a user

[3] Economist Intelligence Unit, "Malaysia Internet: Sub-sector Update," December 20, 2010, http://www.eiu.com/index.asp?layout=ib3Article&article_id=197731004&country_id=1600000160&pubtypeid=1162462501&industry_id=&category_id=&rf=0.

[4] "Internet Reaches One in Five in Malaysia," *Asia Media Journal,* October 23, 2008, http://www.asiamediajournal.com/pressrelease.php?id=610.

[5] Digital Media Across Asia, "Malaysia Internet Penetration: Malaysian Internet Users in Urban/Rural Area," http://comm215.wetpaint.com/page/Malaysia+Internet+Penetration, accessed August 20, 2010.

[6] Malaysia Communications and Multimedia Commission (MCMC), *Communications and Multimedia: Selected Facts and Figures, Q4 2010* (Cyberjaya: MCMC, 2010), http://www.skmm.gov.my/link_file/facts_figures/stats/pdf/Q4%202010%20Text.pdf, accessed February 28, 2011.

[7] Ibid.

8 MCMC, *Communications and Multimedia: Selected Facts and Figures, Q1 2008* (Cyberjaya: MCMC, 2008), http://www.skmm.gov.my/link_file/facts_figures/stats/pdf/Q1.pdf.

[9] MCMC, *Communications and Multimedia: Selected Facts and Figures, Q4 2010.*

posted comments perceived as insulting to the prime minister and Islam.[10]

The lack of high-quality infrastructure in many parts of the country remains the primary obstacle to improved connectivity.[11] In response, the Malaysian government has prioritized the development of broadband internet infrastructure. Broadband usage has increased dramatically since 2007, with household penetration reaching 31.7 percent by the end of 2009. Nevertheless, the infrastructure remains insufficient to meet growing demand.[12] In March 2010, the government launched a National Broadband Initiative, which introduced five programs to expedite expansion of broadband internet and mobile-phone coverage. In some cases, the programs were carried out in cooperation with formerly state-owned Telekom Malaysia, the country's largest telecommunications company, which retains a monopoly over the fixed-line network.[13] In addition to these initiatives, the introduction of wireless WiMAX technology since 2008 has enabled provision of broadband services to areas of the country that are difficult to reach via cable connections; four WiMAX providers were in operation as of mid-2010.

Regulation of the internet falls under the immediate purview of the Malaysian Communications and Multimedia Commission (MCMC), which is overseen by the minister of information, communications, and culture. Both the MCMC and the ministry are guided by the 1998 Communication and Multimedia Act (CMA), which gives the information minister a wide range of licensing and other powers. MCMC commissioners are appointed by the government. Since the end of 2008, the process for appointing members of the MCMC advisory board has become more transparent and participatory, involving consultations with a wide range of stakeholders and resulting in the inclusion of civil society members on the board. The board's powers are extremely limited, however, and the MCMC has emerged as one of the country's greatest obstacles to free expression and a driving force in efforts to censor online speech.

Under the CMA, a license is required to own and operate a network facility. There are 21 ISPs operating in the country, most of them privately owned. There have not been any reported denials of ISP license applications, but the licensing process could serve as a means of control, and the owners of major ISPs and mobile-phone service providers often have connections to the government. Of the two largest ISPs, TMnet and Jaring, the former is a subsidiary of the privatized national phone company Telekom Malaysia, and the latter is wholly owned by the Ministry of Finance. Maxis Communications, the largest mobile-phone service provider, was founded by Ananda Krishnan, who also owns the largest satellite

[10] "Shahidan Wants Facebook Banned, Cites National Security," *Malaysian Insider*, December 6, 2010, http://www.themalaysianinsider.com/malaysia/article/shahidan-wants-facebook-banned-cites-national-security/.
[11] "Your 10 Questions for Dr. Mohamed Awang Lah," *Star Online*, May 22, 2010, http://biz.thestar.com.my/news/story.asp?file=/2010/5/22/business/6298179&sec=business.
[12] MCMC, "Broadband Meter: Subscribers and Users,".*MyConvergence*, March 2010, http://myconvergence.com.my/main/images/stories/SpecialEdition/pdf/MyConBumper_p97_BBMeter.pdf.
[13] Sira Habu and Shaun Ho, "RM 1 Billion Initiative to Promote High-Speed Broadband Usage," *Star Online*, March 25, 2010, http://thestar.com.my/news/story.asp?file=/2010/3/25/nation/5931577&sec=nation.

broadcaster and enjoys close ties to former prime minister Mahathir Mohamad. Two new mobile-phone providers have joined the market since 2008: YTL Communications and Umobile, both of whose owners are closely associated with the ruling party. Since 2007, some local governments, such as those in Selangor and Kuala Lumpur, have sporadically frozen cybercafe licenses or closed venues operating without licenses in an effort to limit illegal activities like online gambling.[14] While it is not part of a deliberate government effort to restrict public access to the internet, the closure of hundreds of cybercafes in this crackdown has hampered access for the general population in some regions of the country.[15]

LIMITS ON CONTENT

The government does not employ any known filtering technology to actively censor internet content, though the authorities have taken other measures to restrict the circulation of certain information. There are no laws aimed at limiting or censoring the internet in particular, and a provision of the CMA explicitly states that nothing in the act "shall be construed as permitting the censorship of the Internet." The Bill of Guarantees of the Multimedia Super Corridor (MSC), an information-technology development project, also promises no censorship of the internet. The government has generally upheld its pledges to avoid direct censorship, except in the case of an MCMC decision to block the controversial website *Malaysia Today* for two weeks in August 2008.[16] The site, founded by popular blogger Raja Petra Kamarudin, has been very critical of the ruling party, but was unblocked following a public outcry.[17]

In August 2009, news emerged that the Information Minister Rais Yatim had directed the MCMC to issue a tender for a nationwide internet filtering system. Following objections from the public and free speech advocates, the plan was put on hold, though it remains unclear whether it has been permanently abandoned.[18] Meanwhile, many government-linked companies and public universities restrict access for their students and employees to certain sensitive websites, such as the independent online news outlet Malaysiakini.

Although there were no reported instances of technical blocking, there have been cases of administrative efforts to remove content from the internet. The energy, water, and communications minister—then responsible for the MCMC before an April 2009 cabinet

[14] Bavani M and Komala Devi, "Illegal Internet Cafés Biting into Business of Legitimate Cybercafés," *Star Online*, May 21, 2010, http://thestar.com.my/metro/story.asp?file=/2010/5/21/central/6304101&sec=central.
[15] Ibid.
[16] "Syed Hamid Tells Why Malaysia Today was Blocked," *Star Online*, August 29, 2008, http://thestar.com.my/news/story.asp?file=/2008/8/29/nation/22194389&sec=nation.
[17] Sim Leoi Leoi and Florence A. Samy, "MCMC Told to Unblock Malaysia Today (Update 2)," *Star Online*, September 11, 2008, http://thestar.com.my/news/story.asp?sec=nation&file=/2008/9/11/nation/20080911145128.
[18] Rebekah Heacock, "Malaysia Considers, Backs Down From National Internet Filter," OpenNet Initiative Blog, August 13, 2009, http://opennet.net/blog/2009/08/malaysia-considers-backs-down-national-internet-filter.

reorganization—reportedly said in September 2008 that the commission had formed a panel composed of the police, officials from the attorney general's office, and representatives of the Home Ministry to monitor websites and blogs. While there is no comprehensive information available, this mechanism appears to be active, as the MCMC has been known to track online discussions and then instruct bloggers or online news outlets to remove articles or comments that are perceived as antiestablishment or overly critical of the government. Procedures surrounding such requests are generally nontransparent. In one case that received widespread attention, the MCMC in September 2009 directed Malaysiakini to take down two videos from its website. The commission argued that the videos were "provocative" and ordered their removal under the CMA. The first video showed Muslim demonstrators marching with a cow's head to protest the relocation of a Hindu temple, and the second showed the home minister defending the protesters. Malaysiakini's editor-in-chief, Steven Gan, refused to comply with the order, stating that his outlet had no ill intentions in posting the videos. Following an investigation that lasted several days and involved the interrogation of multiple staff members, the MCMC forwarded the case to the attorney general, urging that Malaysiakini be prosecuted for failing to comply with the removal order. Should the attorney general pursue the case, Malaysiakini faces a potential fine of up to 50,000 ringgits (US$14,300), and Gan could receive up to a year in prison.[19]

The level of self-censorship appears to have remained consistent in 2009 and 2010 as compared to previous years. Although the repeated prosecution of bloggers has caused some online writers to exercise greater caution, critical commentary and exposés of official misconduct have a regular presence in online discourse. The authorities discourage free expression on sensitive or "red-line" issues such as Islam's official status, race, royalty, and the special rights enjoyed by *bumiputera* (ethnic Malays and other indigenous people, as opposed to the ethnic Chinese and Indian minorities).

Expanded internet access has led to the emergence of a vibrant blogosphere, and an increasing number of Malaysians are turning to the internet as their main source of news. In a survey of the 50 most-viewed websites, Malaysiakini ranked 13th.[20] Despite such popularity, the site has reportedly encountered difficulties securing advertisements, as businesses fear reprisals given the site's reputation for independent journalism and criticism of the government. The use of social-networking platforms has also become a primary online activity for many individuals. There are almost six million Facebook users in Malaysia, and the country is ranked fourth in the Asia-Pacific region for number of social-networking media users.[21] It was also estimated that there were almost 500,000 Twitter users and two

[19] Reporters Without Borders, "Malaysiakini Website Refuses to Bow to Censorship," news release, September 24, 2009, http://en.rsf.org/malaysia-malaysiakini-website-refuses-to-24-09-2009,34575.
[20] Alexa, "Top Sites in Malaysia," http://www.alexa.com/topsites/countries;0/MY, accessed February 23, 2011.
[21] Harmandar Singh, "The Game of Demystifying Social Media," *Star Online*, May 29, 2010, http://biz.thestar.com.my/news/story.asp?file=/2010/5/29/business/6338710&sec=business.

million bloggers as of mid-2010 in Malaysia.[22] Almost all prominent politicians and civil society groups, including those representing ethnic minorities, blog or tweet regularly, and many also have a presence on Facebook, including Prime Minister Najib Razak.[23] English, and to a lesser extent Malay, are the dominant blogging languages.

Some bloggers have exposed corruption in the government or initiated online campaigns to challenge government policies or improve transparency. Penang Watch, launched in 2007, receives and tracks citizens' complaints to the local government in the northern state of Penang in an effort to increase official accountability. In recent years, nearly half of the complaints posted to the site have reportedly been successfully resolved by the local authorities.[24] In October 2010, after the Home Ministry banned a newly released book on Malaysia's leaders, a decision condemned by human rights groups, an alternative copy was circulated online.[25]A loose coalition of bloggers has formed in an effort to self-regulate and advocate against restrictions on free expression. Although they have held annual meetings to discuss ongoing political developments in Malaysia,[26] they have been relatively ineffective due to a lack of formal organization and mechanisms for punishing offending bloggers other than expulsion from the coalition.[27]

VIOLATIONS OF USER RIGHTS

Malaysia's constitution provides each citizen with "the right to freedom of speech and expression," but allows for limitations on this right. The government exercises tight control over print and broadcast media through restrictions on licensing and the use of the Official Secrets Act (OSA), the Sedition Act, and harsh criminal defamation laws to penalize journalists and other critics. Violations of these laws are punishable by several years in prison. With regard to online expression, the government has, on multiple occasions, circumvented protections afforded by the MSC Bill of Guarantees and the CMA,[28] carrying out arbitrary

[22] Yung-Hui Lim, "105,779,710 Users and New Estimates of Twitter Users in Asia," *GreyReview,* April 20, 2010, http://www.greyreview.com/2010/04/20/105779710-million-users-and-new-estimates-of-twitter-users-in-asia/; "Rais: 2 Million Bloggers Proves media Freedom," *Malaysian Digest*, June 17, 2010, http://www.malaysiandigest.com/entertainment-lifestyle/4742-rais-2-million-bloggers-proves-media-freedom.html.

[23] Najib Razak's blog, *1Malaysia*, can be found at http://www.1malaysia.com.my/.

[24] Sopheap Chak, "Penang Watch," Technology for Transparency Network, February 25, 2010, http://transparency.globalvoicesonline.org/project/penang-watch.

[25] Jerrenn Lam, "Malaysia: Home Ministry Bans Controversial Book," Global Voices, October 4, 2010, http://globalvoicesonline.org/2010/10/04/malaysia-home-ministry-bans-controversial-book/.

[26] "Malaysia's Bloggers Debate 'Allah' Issue," Union of Catholic Asian News, May 24, 2010, http://www.ucanews.com/2010/05/24/muslim-bloggers-debate-%E2%80%98allah%E2%80%99-issue/.

[27] Ahirudin Bin Attan, "National Alliance of Bloggers Set Up," *Rock'y Bru* (blog), April 5, 2007, http://rockybru.com.my/2007/04/national-alliance-of-bloggers-set-up.html.

[28] Multimedia Super Corridor (MSC), "MSC Malaysia 10-Point Bill of Guarantees," http://www.mscmalaysia.my/topic/MSC+Malaysia+Bill+of+Guarantees, accessed November 16, 2010; MCMC, "Communications and Multimedia Act 1998," http://www.skmm.gov.my/index.php?c=public&v=art_view&art_id=43,

arrests and launching investigations against internet users under the older, more restrictive laws that had principally been applied to traditional media. In 2009 and 2010, the government also sought to restrict online expression under the CMA itself, particularly relying on the broadly worded Section 233, which bans content deemed "indecent, obscene, false, threatening, or offensive."[29]

Throughout 2009 and 2010, a number of bloggers faced legal harassment, intimidation, fines, and brief periods of detention. No bloggers were imprisoned at year's end, though several had charges pending against them. Bloggers who had been targeted earlier also continued to face legal proceedings, and some new charges were issued. Raja Petra, the blogger and *Malaysia Today* founder, was charged with sedition and criminal defamation in 2009 over his writings implicating the prime minister and his wife in the killing of a Mongolian national. He left the country halfway through his trial, and warrants were issued for his arrest.[30] The charges against him were dropped pending his return to Malaysia. In 2010, new police reports were filed against Petra for his continued criticism of the government from exile,[31] with many ruling party leaders calling for him to be extradited and put on trial. Some have also called for his citizenship to be revoked.[32] In another case, musician Wee Meng Chee, also known as NameWee, was investigated in August 2007 for a parody of the national anthem that was posted on YouTube, and faced another probe in 2009 for criticizing national power supplier Tenaga Nasional over a blackout. In August 2010, police reportedly visited Wee late at night, allegedly as part of an investigation of sedition charges for a video he had posted on YouTube criticizing a school principal for expressing racist slurs about her students.[33]

Over the last two years, several individuals have also been arrested and charged with sedition under the CMA for comments posted in blogs,[34] and for alleged threats made on Facebook.[35] Many of these cases involve individuals who had been critical of Malaysian

accessed November 16, 2010.

[29] Reporters Without Borders, "Malaysiakini Website Refuses to Bow to Censorship."

[30] Teh Eng Hock, "Raja Petra Can't Be Tried in Britain," *Star Online*, May 26, 2010, http://thestar.com.my/news/story.asp?file=/2010/5/26/nation/6340987&sec=nation.

[31] K Kabilan, "RPK: 1Malaysia Will Be Najib's Downfall," *Free Malaysia Today*, May 25, 2010, http://politicalwatchmalaysia.blogspot.com/2010/05/rpk-1malaysia-will-be-najibs-downfall.html "Perkasa Makes Police Report Against Raja Petra," *Malaysia Today,* January 7, 2010; http://malaysia-today.net/mtcolumns/newscommentaries/29452-perkasa-makes-police-report-against-raja-petra.

[32] "Revoke RPK's Citizenship, Government Urged," *Star Online*, May 30, 2010, http://thestar.com.my/news/story.asp?file=/2010/5/30/nation/6369336&sec=nation.

[33] "High-Voltage Insult of TNB Lands Namewee in Trouble," Malaysiakini, November 24, 2009, http://www.malaysiakini.com/news/118254; Lim Kit Siang, "Why Police Investigating Wee Meng Chee for Sedition When There is Nothing Seditious in his Latest 3-Minute Rap Against the Kulai Secondary School Principal for Making Racist Slurs Against Students?," *Lim Kit Siang* (blog), August 31, 2010, http://blog.limkitsiang.com/2010/08/31/why-police-investigating-wee-meng-chee-for-sedition-when-there-is-nothing-seditious-in-his-latest-3-minute-rap-against-the-kulai-secondary-school-principal-for-making-racist-slurs-against-students/.

34 Charles Ramendran, "Bomb Threat by Blogger," *Sun2Surf*, January 13, 2010, http://www.sun2surf.com/article.cfm?id=42322.

[35] G Vinod, "PAS Member: I Did Not Threaten to Kill Saiful," *Free Malaysia Today*, May 19, 2010,

royalty. In early 2009, a constitutional crisis erupted in the state of Perak, where the opposition had gained control in the 2008 elections. Due to defections to the BN, the two sides became evenly divided in the state legislature, both claiming the right to govern. Perak's head of state, Sultan Azlan Shahmade, subsequently made a crucial decision that allowed the BN to regain control of the state government, prompting some internet users to criticize the sultan. Among them were two bloggers, Ahiruddin Attan, known online as Rocky Bru, and Jed Yoong, a former writer for the opposition Democratic Action Party's publication *Rocket*. They were questioned by police in February 2009 over their critiques of the monarchy, but were quickly released.[36] In March of that year, eight more people were charged for making online comments that allegedly insulted the Perak royal family under Section 233(1) of the CMA and Section 34 of the penal code. One of the individuals pleaded guilty and was sentenced to a fine of 10,000 ringgits (US$2,700) or, in default, five months in jail.[37] The spate of cases marked the first time the CMA had been used to charge individuals for comments posted online, setting a precedent that continued to play out in 2010. In January, blogger Khairul Nizam Abdul Ghani was charged with sedition under the CMA for posting comments that insulted a deceased state ruler. He faced a maximum penalty of one year in prison and a fine of up to 50,000 ringgits (US$13,500).[38]

In some cases, bloggers faced legal harassment for content that most observers regarded as humorous satire. On September 24, 2010, police arrested cartoonist Zulfiklee Anwar Ulhaque, better known as Zunar, under the country's Internal Security Act, for publishing cartoons that were deemed insulting to the prime minister and his deputy. Police seized more than 60 copies of a newly published book of his cartoons and raided the offices of Malaysiakini, where Zunar works. Zunar was released soon after his arrest and no formal charges were pressed, though they could be revived at any time.[39] As of the end of 2010, he was reportedly attempting to sue the authorities for unlawful detention.[40] Another blogger, Irwan Abdul Rahman, was charged by the MCMC for circulating false news over a satirical blog post claiming that Malaysia's main utility company was planning to sue the World Wildlife Fund for its Earth Hour initiative, in which individuals are requested to turn off all

http://www.freemalaysiatoday.com/fmt-english/news/general/5771-pas-member-i-did-not-threaten-to-kill-saiful.

[36] Centre for Independent Journalism, "Debate on Royal Powers Draws Attacks and Threats; Bloggers Ahiruddin Attan and Jed Yoong Questioned by Police," International Freedom of Expression eXchange (IFEX), March 4, 2009, http://www.ifex.org/malaysia/2009/03/04/capsule_report_debate_on_royal/.

[37] Centre for Independent Journalism, "Six People Charged with 'Insulting' Royalty Online," IFEX, March 16, 2010, http://www.ifex.org/malaysia/2009/03/16/six_people_charged_with_insulting/; IFEX, "Government Hounds Bloggers That Criticise Royalty," news release, March 25, 2009, http://www.ifex.org/malaysia/2009/03/25/government_hounds_bloggers_that/.

[38] "Malaysian Blogger Charged with Insulting Dead Sultan," *China Post,* January 31, 2010, http://www.chinapost.com.tw/asia/malaysia/2010/01/31/243065/Malaysian-blogger.htm.

[39] "Malaysian Cartoonist Goes into Hiding After Sedition Arrest," RFI English, September 28, 2010, http://www.english.rfi.fr/asia-pacific/20100928-malaysian-cartoonist-goes-hiding-after-sedition-arrest.

[40] Tom Spurgeon, "CR Holiday Interview #7: Zunar," *The Comics Reporter*, December 27, 2010, http://www.comicsreporter.com/index.php/cr_holiday_interview_7_zunar/.

lights and electrical appliances for one hour.[41] He was released on bail, and the court date was set for March 2011. If found guilty, Rahman could be fined up to 50,000 ringgits (US$13,500) or be sentenced to a year in jail.[42]

Two other cases involved complaints over content related to religion or corruption allegations. On August 9, 2010, the right–wing group Perkasa lodged a complaint against blogger Helen Ang for authoring an article that questioned the position of Islam in Malaysia.[43] In October, Malaysia's minister for Information, Communication and Culture lodged a police complaint against two bloggers who alleged that the minister's son had received part of the ministry's1 billion ringgits (US$ 320 million) allocated for improving broadband access in the country.[44] The minister denied the allegations.

The extent of government surveillance of the internet is unclear. However, in recent years the authorities have repeatedly hinted that they may take steps to register bloggers. The information minister floated the idea in May 2009 and again in January 2010, but it was temporarily set aside following protests by the blogging community and several media outlets. Privacy protections are generally poor in Malaysia, and the Internal Security Act allows police to search and seize evidence without a warrant.[45] The authorities appear to be capable of tracking down anonymous internet and mobile-phone users with the help of service providers. Indeed, ongoing court cases indicate that police regularly gain access to the content of text messages from telecommunications companies, sometimes without needing to go through judicial channels. Beginning in 2007, all mobile-phone users, including roughly 18 million prepaid users, were required to register as part of an effort to decrease rumor-mongering activities,[46] though the rule appears to have been weakly enforced. Users in cybercafes are not required to register.

While bloggers and online journalists have been subject to arbitrary arrest, they generally do not face physical violence. However, independent online news outlets and some opposition-related websites faced repeated distributed denial-of-service (DDoS) attacks in 2009 and 2010. Although the attacks have not been conclusively traced to the government, some observers believe that they are either sponsored or condoned by Malaysian security agencies. The *Malaysia Today* website reportedly faced two such attacks in 2009 and another two in 2010, with each crippling the site for four to six hours. A new website, *Free Malaysia*

[41] Reena Raj, "MM Editor Charged for Poking Fun at TNB," Malay Mail, September 2, 2010, http://www.mmail.com.my/content/48276-mm-editor-charged-poking-fun-tnb.
[42] Hafizah Hoze Rizal, "Blogger Hassan Skodeng's Case Set for March 15," Malay Mail, January 26, 2011, http://www.mmail.com.my/content/62051-blogger-hassan-skodengs-case-set-march-15.
[43] "Perkasa Lodges Report Against Blogger," Malaysian Insider, August 9, 2010, http://www.themalaysianinsider.com/malaysia/article/perkasa-lodges-report-against-blogger/.
[44] Cecilia Victor, "Rais Yatim Lodges Report Over Allegations Against Son," Malay Mail, October 12, 2010, http://www.mmail.com.my/content/52046-rais-yatim-lodges-report-over-allegations-against-son.
[45] Privacy International, "Privacy in Asia: Final Report of Scoping Project," November 2009, https://www.privacyinternational.org/issues/asia/privacy_in_asia_phase_1_report.pdf.
[46] "Dec 15 Registration Deadline Stays: MCMC," Bernama, August 18, 2006, http://www.bernama.com/kpdnhep/news.php?id=214811&lang=en, accessed March 20, 2009.

Today, launched in November 2009, was subject to multiple attacks throughout 2010.[47] Similarly, oppositionist websites such as the official site of the People's Justice Party and the blog of its leader, Anwar Ibrahim, suffered DDoS attacks in 2010.[48]

[47] "FMT Comes Under DDOS Attack," *Free Malaysia Today*, April 7, 2010, http://freemalaysiatoday.com/fmt-english/news/general/4294-fmt-comes-under-ddos-attack.
[48] Neville Spykerman, "Cyber Attack: Anwar's Blog Latest to Be Hit," Malaysia Today, September 10, 2010, http://www.malaysia-today.net/mtcolumns/newscommentaries/34410-cyber-attack-anwars-blog-latest-to-be-hit.

MEXICO

	2009	2011
INTERNET FREEDOM STATUS	n/a	Partly Free
Obstacles to Access	n/a	12
Limits on Content	n/a	10
Violations of User Rights	n/a	10
Total	n/a	32

POPULATION: 110.7 million
INTERNET PENETRATION: 28 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

In February 1989, the Autonomous Technological Institute of Monterrey established Mexico's first internet connection.[1] Despite dramatic growth in internet penetration over the last 21 years, the majority of the population, particularly in rural areas, still lacks affordable access. This is largely due to infrastructural deficiencies and high prices resulting from ownership concentration in the telecommunications sector. Nevertheless, access to the internet is expanding, government initiatives are underway to narrow the digital divide, and mobile-phones are widely available.

Once individuals are able to get online, the Mexican internet is predominantly free of censorship, though on several occasions in 2009 and 2010, videos and other content related to political debate were removed at the authorities' behest. While the blogosphere is not as influential as in other countries in the region, the social-networking site Facebook and the Twitter microblogging service have emerged as important tools for citizen mobilization, including in response to drug-related violence and attacks on journalist. Despite the growing violence against traditional media workers, online journalists and bloggers have yet to be similarly targeted.

[1] Network Information Center (NIC) Mexico, "Historia de NIC Mexico" [History of NIC Mexico], http://www.nic.mx/es/NicMexico.Historia (in Spanish), accessed November 16, 2010.

OBSTACLES TO ACCESS

Internet penetration in Mexico has increased significantly over the past decade, from approximately 7.1 million users (8 percent of the population) in 2001 to approximately 30 million (27 percent of the population) in 2010.[2] Nevertheless, these figures remain relatively low for a country at Mexico's level of economic development, and especially for a member of the Organization for Economic Cooperation and Development (OECD). For example, while Mexico has 9.5 internet subscribers for every 100 inhabitants, the OECD average is 20 subscribers for every 100 inhabitants.[3] In addition, technological advancement has been uneven across the country, with a large percentage of users concentrated in Mexico City. In total, 84 percent of users over the age of six reside in urban areas, while only 16 percent live in rural parts of the country.[4] This digital divide is largely due to a lack of infrastructure, reflected in the fact that only 18.4 percent of households have internet service.[5] Together with the high prices described below, this has put the internet beyond the reach of a majority of the population. Nevertheless, cybercafes are generally easy to access in small cities, some small towns, and in areas frequented by tourists. The number of Mexicans accessing the internet primarily at home has increased in recent years, though as of May 2010, 54 percent of users reportedly still accessed the web outside their home.[6] Broadband access is relatively limited. No accurate statistics are available on the level of internet use among the indigenous population.

A lack of competition in the telecommunications sector has contributed to high prices and weakened incentives for the dominant companies to expand services to rural areas, leaving many parts of the country without connectivity. Although there are hundreds of independent internet-service providers (ISPs) in Mexico,[7] the private company Teléfonos de México (Telmex) dominates the market for landlines and DSL broadband internet

[2] International Telecommunication Union (ITU), "ICT Statistics 2001—Internet," http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx, accessed August 30, 2010; "Mexico Online," *eMarketer*, January 2009, http://www.razonypalabra.org.mx/N/n67/varia/oislas/emarketer_2000531.pdf; Internet World Stats, "Internet Usage and Population in Central America," http://www.internetworldstats.com/stats12.htm, accessed August 25, 2010.

[3] "La SCT invertirá 1,500 MDP para Internet" [The SCT Will Invest 1.5 Billion Pesos for the Internet], CNN Expansión, June 23, 2010, http://www.cnnexpansion.com/economia/2010/06/23/sct-invertira-1500-mdp-en-internet (in Spanish); ITU, "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx, accessed August 30, 2010.

[4] Mexican Internet Association (AMIPCI), *Estudio AMIPCI 2009 Sobre Hábitos de los Usuarios de Internet* [AMIPCI 2009 Report on Internet Users' Habits] (Mexico City: AMIPCI, May 2010), http://www.amipci.org.mx/estudios/temp/Estudiofinalversion1110-01989330012742874950B.pdf (in Spanish). Of the 30.6 million users over the age of six, an estimated 25.6 million live in urban areas.

[5] "Sólo el 18% de los hogares en México tienen Internet: INEGI" [Only 18% of Mexican Households Have Internet: INEGI], *El Semanario*, May 17, 2010, http://www.elsemanario.com.mx/news/news_display.php?story_id=38482 (in Spanish).

[6] AMIPCI, *Estudio AMIPCI 2009 Sobre Hábitos de los Usuarios de Internet*.

[7] James Thomasson, William Foster, and Laurence Press, *The Diffusion of the Internet in Mexico* (Austin: Latin American Network Information Center, University of Texas, 2002), http://lanic.utexas.edu/project/etext/mexico/thomasson/thomasson.pdf.

services, providing service to 6.3 million of the latter market's 8 million subscribers.[8] Nevertheless, the cost of a broadband connection remains prohibitively expensive for many Mexicans, ranging from 389 pesos (US$30) to 999 pesos (US$78) per month.[9] In cybercafes, the rate for one hour of access ranges from 10 to 15 pesos (US$0.77 to US$1.15), compared with the minimum wage of 50 to 55 pesos (US$3.80 to US$4.20) an hour depending on location.[10] In addition, a 2010 study found that 52 percent of Mexicans surveyed who did not access the internet explained this was because they did not feel it was important, another potential explanation for the country's relatively low penetration rate.[11]

The Mexican government has acknowledged the serious gaps in internet access and shown greater willingness in recent years to address the problem. In April 2009, Congress introduced a proposed Law for the Development of an Information Society. The draft legislation explicitly recognizes the responsibility of the Mexican state to plan and promote the development of access to information and communication technologies (ICTs).[12] In May 2010, the Department of Communications and Transportation also announced an investment of 1.5 billion pesos (US$115.5 million) to extend internet access to neglected regions that private companies have deemed unprofitable.[13] The government plans for the first time to use a national network of fiber-optic cables to connect outlying regions, and allow third parties to offer internet services.[14] As of mid-2010, steps had also begun to expand broadband services to academic institutions across the country,[15] and the department had joined private investors like the Telefónica Foundation to establish "digital clubs" as a means of introducing new media technologies to broader segments of the population.[16]

Applications like Facebook, Twitter, the video-sharing site YouTube, and international blog-hosting services are freely available and growing in popularity. In 2005, users of the Voice over Internet Protocol (VoIP) service Skype complained that Telmex had blocked access to the platform, allegedly because it feared losing revenue from fixed-line

[8] Isabel Ferguson, "Telmex en 'Infinitum,' sólo si ofrece TV" [Telmex in Infinitum only if TV is offered], CNN Expansión, January 26, 2010, http://www.cnnexpansion.com/negocios/2010/01/25/telmex-pide-video-a-cambio-de-internet (in Spanish).
[9] Ibid.
[10] Thomas Black, "Mexico to Raise Minimum Wage 4.85 Percent on Average in 2010," Bloomberg, December 17, 2009, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aDxkLtk91LkA.
[11] Octavio Islas and Fernando Gutiérrez, "Resultados de los Estudio de Hábitos y Percepciones de los mexicanos sobre internet y Tecnologías Aplicadas 2010" [Results for Study of Mexican Habits and Perception on Internet and Applied Technology, 2010], Razón y Palabra, August-October 2010, http://www.razonypalabra.org.mx/N/N73/Varia73/00Islas_V73.pdf (in Spanish).
[12] Special Committee of Congress for the Promotion of Digital Access to Mexicans, "Ley para el desarrollo de la Sociedad de la Información" [Bill to Promote the Development of the Society of Information], 2009, http://jmcane.files.wordpress.com/2009/04/ley-desarrollo-sociedad-de-la-informacion-mexico.pdf (in Spanish).
[13] "Invertirá SCT mil 500 mdp en Internet" [SCT Will Invest 1.5 Billion Pesos for the Internet], *El Universal*, June 23, 2010, http://www.eluniversal.com.mx/notas/689775.html (in Spanish).
[14] Ibid.; Thomasson and others, *The Diffusion of the Internet in Mexico*.
[15] Thomasson and others, *The Diffusion of the Internet in Mexico*.
[16] Secretariat of Communications and Transportation, "Impulsa SCT Campaña Nacional de Inclusión Digital" [SCT National Campaign Promotes Digital Inclusion], news release, August 13, 2010, http://www.sct.gob.mx/despliega-noticias/article/comunicado-de-prensa-no-131-impulsa-sct-campana-nacional-de-inclusion-digital/ (in Spanish).

calls.[17] The company denied that it was deliberately blocking the application.[18] Following a public outcry, the blocking ended, and as of 2010, the Skype service was freely available.

Six private companies, led by Telcel, control the mobile-phone market. Mobile-phone access is significantly more widespread than internet use, with 83.5 million subscribers as of 2009.[19] Some 8 out of 10 households have at least one mobile phone.[20] The penetration rate has grown rapidly, from 52.6 percent in 2006 to over 80 percent in 2010.[21] According to the Federal Telecommunications Commission (COFETEL), this is still a low rate compared with other OECD countries.[22] Access to the internet via mobile phones has also grown in recent years.[23] However, due to the high cost of third-generation (3G) technology handsets, only 10 percent of users can afford the necessary equipment.[24]

Mexico's legal framework for telecommunications is complicated and outdated, as the main legislation on the topic was passed in the 1960s. COFETEL and the Federal Competition Commission (CFC), an antitrust body, are the primary agencies tasked with regulating the telecommunications sector.[25] Observers and press freedom advocates have criticized COFETEL for its lack of independence from the Department of Communications and Transportation and the executive branch. The president directly appoints COFETEL commissioners without the need for Senate approval, and the commission operates with limited transparency. These problems contribute to mistrust of its actions, especially regarding frequency allocations. Nevertheless, there have been no cases of companies being prevented from offering digital-technology services. The CFC has a better reputation, and its head commissioner has demonstrated the will to enforce antitrust legislation, but the

[17] Ben Charny, "Mexican Telephone Operator Under VoIP Fire," CNET News, April 25, 2005, http://news.cnet.com/Mexico-telephone-operator-under-VoIP-fire/2100-7352_3-5681542.html.
[18] Eduardo Arcos, "Se Confirma el Bloqueo a de VoiP por Telmex/Prodigy" [Telmex/Prodigy Blockage of VoIP Is Confirmed], *Alt1040*, April 21, 2005, http://alt1040.com/2005/04/se-confirma-el-bloqueo-de-voip-en-telmex-prodigy (in Spanish).
[19] ITU, "ICT Statistics 2009—Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx, accessed August 31, 2010.
[20] AMIPCI, *Estudio AMIPCI 2009 Sobre Hábitos de los Usuarios de Internet*, 37.
[21] Federal Telecommunications Commission (COFETEL), "Estadísticas: Telefonía Móvil" [Statistics: Mobile Telephony], http://www.cofetel.gob.mx/wb/Cofetel_2008/Cofe_telefonia_movil (in Spanish), accessed August 31, 2010; "Mexico—Mobile Market—Overview, Statistics and Forecasts," Budde Comm, http://www.budde.com.au/Research/Mexico-Mobile-Market-Overview-Statistics-and-Forecasts.html, accessed February 14, 2011.
[22] Claudia Juarez Escalona, "En México Suman 80.8 millones de Móviles" [80.8 Million Mobile Phones in Mexico], *El Economista*, August 19, 2009, http://eleconomista.com.mx/notas-impreso/internacional/2009/08/19/mexico-suman-808-millones-moviles (in Spanish).
[23] Google Sites, "Telefonía 3G: Mexico 3G," http://sites.google.com/site/telefonia3g/mexico-3g (in Spanish), accessed August 31, 2010.
[24] "Altos costos Limitan Penetración de Celulares 3G en Mercado Mexicano" [High Costs Limit Penetration of 3G Phones in Mexican Market], Informador, December 15, 2009, http://www.informador.com.mx/economia/2008/63021/6/altos-costos-limitan-penetracion-de-celulares-3g-en-mercado-mexicano.htm (in Spanish).
[25] COFETEL, "Ambito de Acción" [Scope of Action], http://www.cofetel.gob.mx/wb/Cofetel_2008/Cofe_ambito_de_accion (in Spanish), accessed August 31, 2010; Federal Competition Commission, "¿Qué hacemos?" [What Do We Do?], http://www.cfc.gob.mx/index.php?option=com_content&view=article&id=54&Itemid=6&lang=es (in Spanish), accessed August 31, 2010.

institution remains weak and has limited power to impose sanctions on large companies like Telmex. There are no restrictions on opening cybercafes, though like other businesses they are required to obtain a license to operate.[26]

LIMITS ON CONTENT

The Mexican authorities do not employ any technical methods to filter or systematically curb access to online content, and no legislation restricts the internet as a medium for mass communication. Nonetheless, there have been isolated incidents in which online content in the public interest has been removed at the behest of government agencies. For example, in March 2010, the authorities in Jalisco asked YouTube to take down a video produced by a local civil society organization that criticized a highway construction project in the region; the video was subsequently deleted.[27] In addition, under Mexican law, the Federal Electoral Institution (IFE) is charged with regulating the use of political advertisements and restricting the circulation of overly negative or false portrayals of candidates. In this context, in April 2009, the IFE ordered the incumbent president's National Action Party (PAN) to remove from its website an online game that was highly critical of other political parties.[28] Two months later, following a complaint lodged by the Institutional Revolutionary Party (PRI), the IFE asked YouTube to take down a video attacking Fidel Herrera, the governor of Veracruz. YouTube complied and the video was removed.[29] In another instance, journalist Alejandro Lelo de Larrea reported in April 2010 that a Facebook group he created calling for President Felipe Calderón's sobriety 24 hours a day was deleted, presumably at the request of the government.[30] There have been no reports of proactive content manipulation by either companies or the government.

Although there is extensive self-censorship among journalists working in traditional media, particularly regarding police activity and drug trafficking, the phenomenon is less prevalent among online journalists and bloggers. This is partly because online journalism is not well developed in Mexico, and online writers are less likely to face violent attacks.

Due to a dearth of funding, including a lack of investor interest in internet advertising, it is difficult for individuals and nonprofit initiatives to establish sustainable

[26] "Por qué un Café Internet aún es buen negocio en México" [Why an Internet Café Is Still Good Business in Mexico], InternetCafes.com.mx (blog), July 1, 2010, http://internetcafes.com.mx/2010/07/por-que-un-cafe-internet-aun-es-buen-negocio-en-mexico/ (in Spanish).
[27] Janet Vazquez, "Censura Jalisco Video de Youtube" [Jalisco's Government Censors Youtube], W Radio, July 12, 2010, http://www.wradio.com.mx/nota.aspx?id=1325812 (in Spanish).
[28] "IFE Censura a PAN: Zavala" [Zavala: PAN Is Censored By IFE], W Radio, April 3, 2010, http://www.wradio.com.mx/nota.aspx?id=789606 (in Spanish).
[29] José Gerardo Mejía, "IFE ordena a YouTube retirar spot de Fidel Herrera" [IFE Orders YouTube to Remove a Video of Fidel Herrera], *El Universal*, May 12, 2009, http://www.eluniversal.com.mx/notas/597512.html (in Spanish).
[30] Katia DÁrtigues, "¿Todos contra Brewer?" [Everybody against Brewer?], Vanguardia, April 27, 2010, http://www.vanguardia.com.mx/%C2%BFtodoscontrabrewer?-492495-columna.html (in Spanish).

online media projects. For example, the electronic magazine *Reporte Indigo*, launched in 2007, is now one of Mexico's most innovative and influential political websites, but due to financial constraints it has been forced to begin charging for its content. Nevertheless, the internet has provided space for certain forms of expression that is unavailable elsewhere. Some community radio stations,[31] such as RadioAMLO Puebla, have successfully migrated online after being shut down by the authorities because of Mexico's restrictive legal framework on such outlets.[32] Journalists' organizations have founded Periodistas de a Pié, aimed at countering growing violence against journalists, and México Infórmate, dedicated to promoting transparency and auditing officials' use of state resources.[33] Blogs and politically oriented web portals have not gained significant influence or succeeded in dramatically widening the spectrum of views available to Mexicans beyond the narrow set of opinions found in the concentrated print and broadcast market. This is not due to deliberate government censorship, however, and the Mexican public generally has open access to the full range of national and international news sources.

Many civil society groups have their own sites, and those that cannot afford a website are able to use blogging platforms to provide information on their activities. According to the World Association of Community Radio in Mexico, the internet has been a helpful tool for nongovernmental organizations operating in rural areas, and especially for female activists.[34]

Facebook has emerged as an important instrument for social and political mobilization, as Mexico was home to over 18 million users at the end of 2010, the largest contingent in Latin America and eighth largest in the world.[35] Twitter also has a growing number of registered users, approximately 146,000 as of February 2010.[36] Citizens have used Twitter and Facebook to exchange information about drug-related violence, and to warn local communities about dangerous situations, especially in the northern states.[37] In October 2009, when Congress introduced a plan to impose a 3 percent tax on internet access, users mobilized via a Twitter movement called "Internet Necesario," and Congress

[31] See the website of the World Association of Community Radio–Mexico at http://www.amarcmexico.org/ (in Spanish).
[32] Julio Hernández López, "Cofetel Golpeadora: Silencia Dos Radios Comunitarias" [Cofetel Shuts Down Two Community Radio Stations], *La Jornada*, October 4, 2007, http://www.jornada.unam.mx/2007/10/04/index.php?section=opinion&article=004o1pol (in Spanish).
[33] See the México Infórmate website at http://www.mexicoinformate.org/portal/ (in Spanish).
[34] Interview with Laura Salas, advocacy coordinator for AMARC–México, August 2010.
[35] "Mexico Facebook Statistics," Socialbakers, http://www.socialbakers.com/facebook-statistics/mexico/last-3-months#chart-intervals, accessed February 14, 2011.
[36] "There Are 148,000 Accounts of Mexican Users on Twitter," *Latin Daily Financial News*, February 9, 2010, http://www.latindailyfinancialnews.com/index.php/en/business/mexico/3956-there-are-148-thousand-accounts-of-mexican-users-on-twitter.html; "Twitter en México, algunos numerous" [Twitter in Mexico, some numbers], http://www.webadictos.com.mx/2010/02/08/twitter-en-mexico-algunos-numeros/, accessed February 14, 2011.
[37] Miguel Castillo, "Mexico: Citizen Journalism in the Middle of Drug Trafficking Violence," Global Voices, May 5, 2010, http://globalvoicesonline.org/2010/05/05/mexico-citizen-journalism-in-the-middle-of-drug-trafficking-violence/.

was forced to withdraw the proposal.[38] Finally, in July 2010, the Periodistas de a Pié movement launched a campaign called "Los queremos vivos" to protest attacks against journalists, using Twitter and Facebook to organize rallies and demand government action. The campaign organizers were able to gather approximately 1,000 journalists, with demonstrations taking place in Mexico City, Tijuana, Culiacán, and elsewhere.[39] In advance of federal elections in 2009, a number of NGOs adapted the crowdsourcing platform Ushahidi to track reports of vote-buying by citizens, eventually leading to additional investigations by the special prosecutor.[40] Despite these successes, online activism remains limited to a small community, as many of the most popular bloggers address personal topics rather than engaging in political or social commentary.[41]

In addition to civil society uses of social media tools, all political parties participating in the 2009 elections launched online campaigns to reach potential voters, with some candidates using Twitter or Facebook to communicate their platforms.[42] In a more disturbing trend, drug cartels have also begun using social media applications to exchange information on military checkpoints, prompting calls by some Mexican politicians for increased government monitoring and regulation of these tools.[43]

VIOLATIONS OF USER RIGHTS

The constitution guarantees freedom of speech and freedom of the press. The federal criminal defamation law was repealed in 2007, but civil insult laws remain on the books, and criminal defamation statutes exist in 17 of Mexico's 32 states.[44] During 2009, local press freedom watchdogs reported several cases of harassing lawsuits against journalists,[45] though

[38] Renata Avila, "#InternetNecesario," Technology for Transparency Network, February 13, 2010, http://transparency.globalvoicesonline.org/project/internetnecesario.

[39] National Center for Social Communication, "Cientos marchan por la Libertad de Expression" [Hundreds March for Freedom of Expression], Campaña Permanente, August 9, 2010, http://www.libertad-expresion.org.mx/tag/los-queremos-vivos/ (in Spanish).

[40] Susannah Vila, "Cuidemos el Voto" [Care for the Vote], Technology for Transparency Network, April 27, 2010, http://transparency.globalvoicesonline.org/project/cuidemos-el-voto.

[41] Kaitlyn Wilkins, "Social Media in Mexico: 5 Things You Need to Know," Ogilvy Public Relations Worldwide, September 24, 2009, http://blog.ogilvypr.com/2009/09/social-media-in-mexico-5-things-you-need-to-know/.

[42] Octavio Islas, Amaia Arribas, and Erika Minera, "El empleo propagandístico de Internet 2.0 en campañas a puestos de elección ciudadana, Estado de México, Julio 2009" [The Use of Web 2.0 Propaganda in Campaigns for Elected Office, State of Mexico, July 2009], *Razon y Palabra* 14 no. 70 (November 2009–January 2010), http://www.razonypalabra.org.mx/N/N70/Final_Argentina.pdf (in Spanish).

[43] Alexis Okeowo, "To Battle Cartels, Mexico Weighs Twitter Crackdown," *Time*, April 14, 2010, http://www.time.com/time/world/article/0,8599,1981607,00.html/r:t#ixzz0laM8OTIa.

[44] Article 19, "State of Veracruz Decriminalizes Defamation," International Freedom of Expression eXchange, July 26, 2010, http://www.ifex.org/mexico/2010/07/27/defamation_decriminalised/.

[45] See for example Periodistas en Linea [Online Journalists], "Caso Sosa Castelán vs. Alfredo Rivera Flores y Miguel Angel Granados Chapa," news release, http://www.periodistasenlinea.org/modules.php?op=modload&name=News&file=article&sid=9684 (in Spanish), accessed November 22, 2010.

there have been no such cases lodged against online journalists. A 2009 Supreme Court decision expanded the range of reporting protected from state defamation laws, and some states have gradually followed the federal lead in decriminalization. These positive changes to the legal environment presumably also benefit online journalists and bloggers.

There are no legal provisions enabling the monitoring of internet activity, and online surveillance is not a serious concern in Mexico. However, in recent years, some scandals have emerged in which the authorities recorded mobile-phone calls by politicians or private individuals. In addition, a law passed in 2008 mandated that mobile-phone companies keep a registry of communications and text messages for use by law enforcement agencies in combating extortion and kidnappings.[46] Critics expressed doubt that the authorities would securely store the information to protect users' privacy, especially given past failures by the state to safeguard such data.[47] Nevertheless, 70 percent of users complied with the registration requirement by the deadline, in part due to threats that their line would be cancelled if they did not. The government then extended the deadline, and it was anticipated that most users would be registered by late 2010.

Violence against traditional media journalists has increased sharply since 2006, with reporters probing police issues, drug trafficking, and official corruption facing a high risk of physical harm. According to the Committee to Protect Journalists, at least 22 journalists have been killed in Mexico in connection with their work since 1992.[48] The National Human Rights Commission, which is more liberal in its definition of journalism-related deaths, cites 64 killings since 2000.[49] This phenomenon has been exacerbated by widespread impunity for those carrying out such attacks. While there have been no reports of physical attacks or killings in retaliation for online forms of expression, some prominent bloggers retain their anonymity for fear of potential reprisals.[50]

Cyberattacks are not a serious problem in Mexico, especially compared to other countries in the region like Brazil. However, in July 2010, a Mexican man claimed responsibility for an attack that caused Google searches of the word "vaticano" to be redirected to the website pedifilo.com, as a critique of cases of pedophilia within the Catholic church.[51]

---

[46] "En México Todas las Conversaciones Telefónicas Serán Grabadas y se Guardarán Durante Un Año" [In Mexico, All Telephone Conversations Will Be Recorded and Stored for One Year], *Babel Del Norte*, December 16, 2008, http://www.babeldelnorte.com/index.php?view=article&catid=39%3Acultura&id=719%3Aen-mexico-todas-las-conversaciones-telefonicas-seran-grabadas-y-se-guardaran-por-un-ano (in Spanish).

[47] Miguel Castillo, "Mexico: Fear and Intimidation in Electronic Media," Global Voices, May 12, 2010, http://globalvoicesonline.org/2010/05/12/mexico-fear-and-intimidation-in-electronic-media/.

[48] Committee to Protect Journalists, "22 Journalists Killed in Mexico Since 1992/Motive Confirmed," http://cpj.org/killed/americas/mexico/, accessed August 25, 2010.

[49] "UN, OAS Rips Mexico Over Freedom of Expression," *Latin American Herald Tribune*, August 26, 2010, http://laht.com/article.asp?ArticleId=364380&CategoryId=14091.

[50] Olga R. Rodriguez, "Narco-Blogger Beats Mexico Drug War News Blackout," Associated Press, August 12, 2010, http://www.google.com/hostednews/ap/article/ALeqM5gB8cHuobTuv0x63xhVQURz0zomFQD9HI77O81.

[51] "Mexican Claims Responsibility for Cyber Attack Against Vatican on Google," Catholic News Agency (CAN), July 21, 2010, http://www.catholicnewsagency.com/news/mexican-claims-responsibility-for-cyber-attack-against-the-vatican-on-google/.

NIGERIA

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Partly Free**
Obstacles to Access	n/a	13
Limits on Content	n/a	10
Violations of User Rights	n/a	12
Total	**n/a**	**35**

POPULATION: 158.3million
INTERNET PENETRATION: 28 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

In 1999, Nigeria returned to civilian governance after almost 30 years of military rule.[1] Press freedom and the space for free expression have since increased. Nevertheless, the legal and political environment for traditional media remains harsh, and a number of journalists have been killed in recent years. Online media have been comparatively free from such restrictions to date, though two bloggers were detained for questioning in late 2008. The Nigerian authorities do not carry out any filtering of content, and while access to information technology is still limited for many Nigerians, the number of internet users nearly quadrupled between 2008 and 2010. Several recent legislative initiatives have raised concerns that the relative freedom and privacy enjoyed by online journalists and writers may come under threat in the near future.

The internet was first introduced in the early 1990s, and usage grew more popular following an internet workshop organized by the Yaba College of Technology in 1995.[2] Internet access expanded as cybercafes sprang up in major cities across Nigeria in 1999, though it was still expensive and connections were very slow. The introduction of internet access via mobile-phone service in 2004 spurred further increases in internet use.

[1] Abegunrin Olayiwola, *Nigerian Foreign Policy Under Military Rule, 1966–1999* (Westport, CT: Praeger, 2003).
[2] The workshop was hosted by the Yaba College of Technology in Lagos in collaboration with the Nigerian Communications Commission, the National Data Bank, the Literacy Training and Development Program for Africa (University of Ibadan), the Administrative Staff College of Nigeria (ASCON), the United States Information Service (USIS), the Regional Information Network for Africa (RINAF), and the British Council. United Nations Economic Commission for Africa, "Nigeria: Internet Connectivity," http://www.uneca.org/aisi/nici/country_profiles/Nigeria/nigeriainter.htm, accessed August 27, 2010.

OBSTACLES TO ACCESS

Internet access in Nigeria has grown exponentially in recent years, particularly after the introduction of mobile-phone data services and Fixed Wireless Access (FWA) services. There were about 100,000 users in 1999,[3] but the figure grew to 11 million in 2008,[4] and reached almost 44 million in 2010.[5] This large jump in access is due to an increase in mobile-phone usage and data services over this period, private sector and government investment in technology, and increased competition between FWA providers. Nevertheless, the penetration rate is only 30 percent of the Nigerian population, and access is greater in urban areas than in rural regions. Cost is a key barrier to access for many Nigerians, as the price for internet use ranges from US$1 per hour in cybercafes to an average of US$7 per megabyte of data on Global System for Mobile (GSM) networks. FWA service costs an average of US$80 per month. By comparison, the new minimum wage announced by the government in July 2010 is US$120 per month.[6] Literacy remains an obstacle as well, as 28 percent of the population is illiterate, particularly in English, the main language used by Nigerian online news outlets and blogs.[7]

According to a May 2009 survey of internet users, most Nigerians access the internet from cybercafes or their workplace, while only 17 percent do so from home. Among these users, a large percentage is well educated, with 41 percent holding secondary school degrees and 32 percent holding bachelor's degrees.[8] In recent years, frequent power cuts have become an impediment to internet access, with many users reportedly using private generators to stay online during outages. A number of cybercafes have closed due to difficulties paying for such expensive backup power generation in addition to internet service. The loss of cybercafes has been somewhat offset by the rise of mobile internet usage and affordable packages offered by FWA service providers. Although many providers use the word "broadband" in their promotional materials, in practice there is limited broadband service available in Nigeria, with some estimates placing the number of broadband subscribers as of December 2009 at only 67,800.[9]

[3] Ibid.
[4] "Nigeria Internet Users Tops 11 Million, Penetration Now 7.8%," *Web Trends Nigeria* (blog), October 8, 2009, http://webtrendsng.com/blog/nigeria-internet-users-tops-11-million-penetration-now-7-8/.
[5] Internet World Stats, "Internet Usage Statistics for Africa," http://www.internetworldstats.com/stats1.htm#africa, accessed August 27, 2010.
[6] Funmi Komolafe, "The Road to a New National Minimum Wage," *Vanguard*, July 22, 2010, http://www.vanguardngr.com/2010/07/the-road-to-a-new-national-minimum-wage/.
[7] United Nations Children's Fund, "At a Glance: Nigeria—Statistics," March 2, 2010, http://www.unicef.org/infobycountry/nigeria_statistics.html.
[8] 'Gbenga Sesan, "Digital Lifestyle of Connected Nigerians: Advance Report," Paradigm Initiative Nigeria, March 2010, http://www.pinigeria.org/download/dlcnadvance.pdf.
[9] Internet World Stats, "Africa: Nigeria," http://www.internetworldstats.com/africa.htm#ng, accessed August 27, 2010.

The number of mobile-phone subscribers has increased dramatically over the past decade, from almost no users in 2000 to over 83 million in 2010.[10] Mobile internet penetration has also increased, reportedly reaching 7.3 million users by 2008.[11] While users with any smart phone can access the internet on their mobile devices, specific handsets such as Nokia's *C3* and Research in Motion's *Blackberry* provide bundled data services to mobile subscribers. The number of BlackBerry users appears to be growing, particularly among young Nigerians, though the cost of the service, whose efficiency is limited, remains $20 per month. According to credible sources in the industry, there were approximately 86,500 BlackBerry subscribers with the service providers MTN, Zain, and Etisalat as of July 2010.[12]

Until recently, most businesses requiring high bandwidth—such as internet-service providers (ISPs), banks, and telecommunications companies—relied on satellite links and the SAT-3 undersea cable for their international internet connection. When the SAT-3 cable encountered problems in July 2009,[13] as much as 70 percent of the country's internet traffic was cut off.[14] In March 2007, the government established the Nigerian Internet Exchange Point as a means of connecting ISPs to one another; as of mid-2010, it had 22 members[15]. Several telecommunications companies have also migrated to private fiber-optic cable projects, such as Glo-1 and MainOne. The latter cable went live on July 1, 2010, and now provides connectivity for the ISPs MTN, Etisalat, and Starcomms,[16] though the reduced cost of a cable rather than a satellite connection has yet to be passed on to consumers. Despite media reports in 2009 that the Glo-1 cable had been connected, [17] as of late-2010 it was still not operational.

The video-sharing website YouTube, the social-networking site Facebook, the microblogging application Twitter, and various international blog-hosting services are freely available and among the most popular websites in the country. As of December 2010, there

[10] Nigerian Communications Commission, "Subscriber Data," http://www.ncc.gov.ng/subscriberdata.htm, accessed December 27, 2010.
[11] "Mobile Internet Usage Soars in Nigeria," ITNewsAfrica.com, December 4, 2008, http://www.itnewsafrica.com/?p=1906.
[12] Interviews with employees of MTN, Zain, and Etisalat who requested anonymity, August 2010. Globacom figures were not available at the time of writing.
[13] Efem Nkanga, James Emejo, and Chinwe Ochu, "Nigeria: Damage to SAT-3 Cable Cripples Banks, Internet Services," *This Day*, July 29, 2009, available at http://allafrica.com/stories/200907290153.html.
[14] "Damage to SAT-3 Cable Disrupts Internet Services in Nigeria," *Afrique en Ligne*, July 29, 2009, http://www.afriquejet.com/news/africa-news/damage-to-sat-3-cable-disrupts-internet-services-in-nigeria-2009072932548.html.
[15] Internet Exchange Point of Nigeria, "Our Members," http://www.nixp.net/index.php?option=com_content&view=article&id=13&Itemid=13, accessed December 29,2010.
[16] Sean Buckley, "Main One Cable Rakes in Three Carrier Customers," *Fierce Telecom,* July 22, 2010, http://www.fiercetelecom.com/story/main-one-cable-rakes-three-carrier-customers/2010-07-22.
[17] Rebecca Heacock, "Nigeria: New Submarine Internet Cable Lands in Lagos," *Global Voices,* September 7, 2009, http://globalvoicesonline.org/2009/09/07/nigeria-new-submarine-internet-cable-lands-in-lagos; Prince Osuagwu, "Glo 1 Submarine Cable Lands in Lagos," *Vanguard*, September 6, 2009, http://www.vanguardngr.com/2009/09/06/glo-1-submarine-cable-lands-in-lagos.

were reportedly 2.1 million Facebook users.[18] According to Alexa, a website rating company, the 10 most popular websites in Nigeria as of mid-2010 were Yahoo!, Facebook, Google.com, Google.com.ng, Blogger.com, Live.com, YouTube, Wikipedia, Nairaland (a Nigerian online discussion forum), and Twitter.[19] Three other Nigerian websites—*Punch* newspaper at number 13, GTBank at number 18, and *Vanguard* newspaper at number 20—were cited in the top 20. The growing demand for advanced web applications has sparked multiple local clones of internationally known services.

The information and communication technology (ICT) market in Nigeria has expanded significantly over the past decade. The number of ISPs has risen from 18 in 2000 to 151 licensed and active providers as of mid-2010,[20] as well as 14 active FWA providers,[21] and four GSM mobile-phone operators that also provide internet access to their subscribers.[22] A recent study that analyzed data from 2,069 internet users across Nigeria found the leading service providers to be Globacom, MTN, Starcomms, Zain, and Multilinks.[23] Globacom, MTN, and Zain are GSM service providers, while Starcomms and Multilinks are FWA service providers. All of the above companies are privately owned. The only government-owned firm in the market, NITEL, is not particularly competitive. It has remained on the government's privatization list for several years following multiple attempts to sell it. In February 2009, Transcorp, a local conglomerate with strong ties to the government, relinquished its 51 percent stake, which it had acquired in 2006.[24] In February 2010, New Generation Telecoms, a consortium that includes China Unicom, won a controversial bid to purchase the company.[25] Responding to allegations of corruption surrounding the purchase, the president initiated an investigation, and as of mid-2010 the transaction had yet to be concluded.[26]

Internet services are governed by the Nigerian Telecommunications Act, which vests regulatory responsibilities in the Nigerian Communications Commission (NCC). All ISPs must obtain a license from the NCC to operate, but there have been no reports of any ISP

[18] Facebakers, "Facebook Statistics Nigeria," http://www.facebakers.com/countries-with-facebook/NG/, accessed December 29, 2010.
[19] Alexa Web Information, "Top Sites in Nigeria," http://www.alexa.com/topsites/countries/NG, accessed August 27, 2010.
[20] Nigerian Communications Commission, "Internet Services," http://www.ncc.gov.ng/Licensees/Licensees-Internet_Services.pdf, accessed December 31, 2010.
[21] Nigerian Communications Commission, "Fixed Wireless Access," http://www.ncc.gov.ng/list_of_licensees/Current/Fixed_Wireless_Access.pdf, accessed August 27, 2010.
[22] Nigerian Communications Commission, "Digital Mobile License," http://www.ncc.gov.ng/list_of_licensees/Current/Digital_Mobile_License.pdf, accessed August 27, 2010.
[23] Sesan, "Digital Lifestyle."
[24] Transcorp, "NITEL Board Ratifies Appointment of Chairman: About NITEL," September 24, 2008, http://www.transcorpnigeria.com/corporatecom/archives.php?page=fullstory&nid=60; Betrand Nwankwo and Juliet Alohan, "Nigeria: Transcorp Relinquishes 51 Percent Equity Share in Nitel/Mtel," *Leadership*, February 26, 2009, available at http://allafrica.com/stories/200902260498.html.
[25] Camillus Eboh, "New Generation Telecoms Acquires NITEL," Reuters, February 16, 2010, available at http://234next.com/csp/cms/sites/Next/Home/5527697-146/new_generation_telecoms_acquires_nitel_.csp.
[26] Camillus Eboh, "Nigeria Cabinet Sacking Delays Nitel sale," Reuters, March 19, 2010, http://www.reuters.com/article/idUSLDE62I0WS20100319.

being denied a license or renewal of registration. However, new ISPs seeking to enter the market have faced challenges in their operations due to competition from larger ISPs and investor focus on the mobile sector. Although the NCC's nine-member board is nominated by the government, the regulator's decisions are viewed as relatively independent.

LIMITS ON CONTENT

The Nigerian government has not been reported to engage in any form of internet filtering.[27] According to a study by the OpenNet Initiative, several websites were inaccessible surrounding elections in 2007. However, the researchers concluded that the disruptions were due to technical problems, not government intervention.[28] The complex nature of Nigeria's internet framework as described above makes it difficult to carry out systematic filtering or censorship. Some ISPs have been known to block access when users infringe on laws by downloading copyrighted content, but this has been done to manage network traffic rather than protect intellectual property.

In June 2009, reports emerged that the Nigerian government planned to invest in sponsoring pro-government websites and blogs.[29] In practice, it has not been possible to confirm whether the plan was implemented. Websites, blogs, and commentators are generally divided among anti-government, pro-government, and neutral leanings, and this has continued as online political discussions have increased in advance of polls scheduled for April 2011.

The country is home to a diverse blogosphere, with entertainment blogs drawing the most readers and a growing number of Nigerians blogging about their personal lives or social activism. Blogs have gradually emerged as an important platform for discussion and a source of reliable news for many users. Readers often leave comments on popular news-oriented blogs to express their frustration with societal ills. Although traditional media outlets often shy away from sensitive topics, such as late president Umaru Yar'Adua's declining health, such topics are addressed freely online, with commentary ranging across blogs, Facebook, and Twitter. The Nigerian blogosphere includes both Nigerians living abroad and locally based writers. While many of the former are longtime bloggers, only in the past five years have Nigerian residents actively joined the blogosphere,[30] with local

[27] OpenNet Initiative, "Country Profile: Nigeria," October 1, 2009, http://opennet.net/research/profiles/nigeria.
[28] OpenNet Initiative, "Internet Watch Report: The 2007 Presidential Elections in Nigeria," November 2007, http://opennet.net/research/bulletins/014.
[29] Global Voices, "Nigeria government launches attack against bloggers,", June 25, 2009, http://advocacy.globalvoicesonline.org/2009/06/25/nigeria-government-launches-attack-against-bloggers/; Sahara Reporters, "Umaru Yar'adua Regime Launches $5 Million Online War," June 16, 2009, http://www.saharareporters.com/news-page/umaru-yar%E2%80%99adua-regime-launches-5-million-online-war.
[30] Remmy Nweke, "Nigeria: Blogging as a Trend in Nigeria," *Daily Champion*, January 12, 2006, available at http://allafrica.com/stories/200601120144.html.

blogging gaining momentum following a 2008 Nigerian bloggers' conference.[31] Although two attempts to create Nigerian blog aggregators failed,[32] GlobalVoicesOnline.org, Blogger.com, Afrigator.com, and WordPress.com are popular platforms for Nigerian bloggers to interact and learn from one another. The popularity of blogs has influenced the traditional media environment, with major newspapers adding interactive features to their websites. For example, 6 of the 10 most visited Nigerian websites as of July 2010 are owned by newspapers that have embraced the blogging culture.[33]

ICTs have also played an important role in mobilizing people for "real life" protests and providing updates on unfolding events. In November 2008, a widely circulated YouTube video showed an admiral and several other military officers severely beating a woman who they deemed too slow in making way for their convoy.[34] Following a public outcry, and with legal aid from the state government, the woman sued the officers for assault and battery. In January 2010, a court awarded her 100 million naira (US$670,000) in compensation.[35] In another instance, BlackBerries were a key factor in galvanizing thousands of young professionals for a March 2010 political rally held in Abuja, Nigeria's capital, to protest a wide range of problems, including poor infrastructure, fuel shortages, and power blackouts.[36] Civil society groups and candidates are also using new media tools ahead of Nigeria's 2011 elections. Popular citizen-initiated campaigns include the Save Nigeria Group,[37] the Enough Is Enough Nigeria coalition,[38] and the "Nigerians Say No to Ibrahim Babangida as President" Facebook group.[39] Prospective presidential candidates such as celebrity journalist Dele Momodu, former governor Donald Duke, former military ruler Ibrahim Babangida,[40] and the current president are using websites, mobile-phone text messages, e-mail, Twitter, and Facebook to reach potential voters and run their campaigns. Particularly notable during the latter part of 2010 was President Goodluck Jonathan's use of

[31] Gbenga Sesan, "The Nigerian Bloggers' Forum," *Oro* (blog), September 22, 2005, http://www.gbengasesan.com/blog/?p=10.
[32] The Nigerian Blog Aggregator was available at http://www.nigerianbloggers.com and the Nigerian Weblog Ring was at http://nwr.cowblock.net.
[33] "Most Visited Nigerian Websites in July 2010," *Web Trends Nigeria*, August 9, 2010, http://webtrendsng.com//blog/most-visited-nigerian-websites-in-july-2010.
[34] *Brutalization of Uzoma Okere* (YouTube, November 10, 2008), 1 min., 40 sec., http://www.youtube.com/watch?v=VHdkyvn41us.
[35] "Uzoma Okere Won N 100 Million," *Nigerian Curiosity* (blog), January 29, 2010, http://www.nigeriancuriosity.com/2010/01/uzoma-okere-won-n100-mn-video.html.
[36] Stephanie Busari, "Rare Anger as Nigerian Youth Hit Streets," CNN, March 16, 2010, http://edition.cnn.com/2010/WORLD/africa/03/16/nigeria.youth.protests/index.html.
[37] The group's website is located at http://www.savenigeriagroup.com.
[38] The coalition's website is located at http://www.enoughisenoughnigeria.com.
[39] "Nigerians Say No to Ibrahim Babangida as President," Facebook, http://www.facebook.com/pages/YOUTH-SAY-NO-TO-EVIL-GENIUS-IBB-IN-2011/114209978613655#!/group.php?gid=116661691680343&ref=ts.
[40] These three men's campaign-related websites are located at http://www.delemomodu2011.com, http://www.donalddukeorganisation.org, and http://www.voteibb.org, respectively.

Facebook, earning him the label "Facebook President."[41] The president's daily profile updates emerged as a popular avenue for public engagement. Citizen comments to the page have been known to influence high-level policy making, such as a July 2010 decision to reverse a ban on the country's football team.[42] Similarly, the president's formal declaration of his candidacy for the 2011 electoral race was first announced on Facebook.[43] In December 2010, he released a book compiling his interactions with citizens via the social-networking website.[44]

VIOLATIONS OF USER RIGHTS

Nigeria's legal framework is fairly archaic, as many laws have not been updated to reflect modern realities, including the use of new media technologies.[45] This lack of internet-specific legislation has generally fostered an open environment for online activities. In recent years, the government has introduced several bills that could be used to restrict users' rights to free expression and privacy, though their passage in the near future is unlikely due to the expected elections in early 2011. Much of the public accepts the need for some regulation of internet use in light of the unchecked cybercrime in the country, and the costs it has imposed on Nigeria's economy and global reputation.

The 1999 constitution guarantees freedom of expression and of the press, but the state often uses arbitrary and extralegal measures to suppress political criticism in the media, and there is a culture of impunity for crimes against media workers. Libel remains a criminal offense, and the burden of proof rests with the defendant. Journalists covering sensitive issues such as official corruption, the president's health, and communal violence are regularly subjected to criminal prosecution. However, no such cases have yet been brought for online expression.[46] The implementation of Sharia (Islamic law) penal codes in 12 northern states has generally not affected internet freedom. However, in March 2010, a

[41] George Webster, "Goodluck Jonathan: The Facebook President," October 1, 2010, http://articles.cnn.com/2010-10-01/tech/goodluck.jonathan.facebook.profile_1_facebook-fans-popular-social-networking-site-nigerian-president.
[42] "Facebook influences Nigeria football team ban U-turn," British Broadcasting Network (BBC), July 6, 2010, http://www.bbc.co.uk/news/10525699.
[43] "Formal Declaration of Dr Jonathan Ebele Goodluck For President 2011," Nigerians For Goodluck/Sambo Ticket on Facebook, http://www.facebook.com/topic.php?uid=147860418583907&topic=210, accessed February 11, 2010.
[44] David Olagunju, "Between Jonathan and his friends," *Nigerian Tribune*, January 3, 2010, http://tribune.com.ng/index.php/politics/15546-between-jonathan-and-his-friends.
[45] For example, the Evidence Act does not provide for the acceptance of digital evidence in court, although an appellate court in Lagos ruled in May 2010 that computer-generated bank statements could be admitted in the graft trial of a former minister. Patience Akpuru, "Nigeria: Fani-Kayode Appeal Court Admits Computer Print-Out," *Daily Champion*, May 28, 2010, available at http://allafrica.com/stories/201005310338.html.
[46] Karin Karlekar, ed., "Nigeria," in *Freedom of the Press 2009* (New York: Freedom House, 2009), http://www.freedomhouse.org/inc/content/pubs/pfs/inc_country_detail.cfm?country=7675&year=2009&pf.

Sharia judge in Kaduna state banned efforts by the Civil Rights Congress of Nigeria to initiate online discussion of an amputation sentence on Facebook and Twitter.[47]

The Nigerian authorities have a history of arresting and intimidating traditional media workers, and at least eight journalists have been killed in connection with their work since 1998.[48] Although no individuals had been sentenced to prison or physically attacked for online activities as of mid-2010, security agencies in late 2008 detained and interrogated two overseas bloggers upon their arrival in Nigeria. Jonathan Elendu, author of the website Elendu Reports, was arrested in October 2008 by the State Security Service, which is known to take orders directly from the president. He was reportedly questioned in relation to national security issues and for "sponsoring a guerrilla news agency."[49] Many observers believed he was detained due to an alleged connection with another online platform, Sahara Reporters, that published photographs of President Yar'Adua's 13-year-old son "waving wads of money around and holding a policeman's gun,"[50] or for falsely reporting during the 2007 presidential election campaign that Yar'Adua had died. Elendu was released after two weeks without facing charges.[51] The following month, another U.S.-based online journalist, Emmanuel Emeka Asiwe, editor of the Huhuonline website, was detained. The State Security Service similarly stated that Asiwe was being questioned about "matters of national security," and released him after a week of interrogation.[52]

Nigerian security services do not appear to monitor internet and mobile-phone communications, but many online journalists suspect that they are being monitored by the state. In addition, lawmakers are currently considering measures that could pave the way for comprehensive surveillance. One bill that has raised concerns among free expression advocates is the Cyber Security and Information Protection Agency Bill, introduced in January 2009 and still pending as of mid-2010. Section 29(2) of the bill includes a vague provision that grants power to any law enforcement officer—upon a "reasonable suspicion that an offence has been committed"—to decrypt data or require the holder of subscriber or

[47] The case centered on Buba Bello Jangebe, whose hand was amputated in 2000 as punishment for stealing a cow. See Imam Imam, "Nigeria: Sharia Judge Bans Amputation Discussion on Facebook, Twitter," *This Day*, March 24, 2010, available at http://allafrica.com/stories/201003240460.html; "Civil Right Congress—Nigeria," Facebook, http://www.facebook.com/group.php?gid=372845616580; Shehu Sani, "CRC Condemns the Amputation of Buba on March 22, 2000," Twitter, March 30, 2010, http://www.twitter.com/shehusani.

[48] Committee to Protect Journalists, "8 Journalists Killed in Nigeria Since 1992/Motive Confirmed," http://www.cpj.org/killed/africa/nigeria/, accessed August 27, 2010.

[49] Ndesanjo Macha, "Nigerian Blogger Arrested for Sponsoring a 'Guerilla News Agency,'" Global Voices, October 24, 2008, http://globalvoicesonline.org/2008/10/24/nigerian-blogger-arrested-for-sponsoring-a-guerilla-news-agency.

[50] "News Blogger Detained in Nigeria," British Broadcasting Corporation (BBC), October 23, 2008, http://news.bbc.co.uk/1/hi/world/africa/7686119.stm. Sahara Reporters stated that Elendu was not on their staff and had nothing to do with the photos.

[51] Reporters Without Borders, "Nigeria: Online Journalist Emmanuel Emeka Asiwe Freed After One Week," news release, November 18, 2008, available at http://allafrica.com/stories/200811181177.html.

[52] Ibid.

traffic information to share relevant details and related content.[53] There are similar provisions in the Mobile Phone Registration Bill,[54] and in the Electronic Fraud Prohibition Bill,[55] introduced to the National Assembly in July 2008. As mentioned above, as of December 2010, discussion and passage of these bills had been put on hold given the shifted focus of politicians on expected elections in 2011. As part of efforts to crack down on cybercrime, law enforcement officers have been known to raid cybercafes and randomly stop drivers to ask youth why they have laptops or printed documents (especially e-mail messages) in their possession.

Cybercafes do not require customers to register or present any form of identification, and any "monitoring" software installed on their computers is used only for billing purposes. In June 2009, drawing on the 2003 Nigerian Communications Act, the NCC announced that mobile-phone companies would be expected to register all SIM cards by March 1, 2010 (later postponed to May 1, 2010).[56] Although the registration process has commenced, implementation has been slow.

Cybercrime, particularly online fraud and spamming, is a serious problem in Nigeria. Between 2002 and 2009, the country repeatedly appeared among the top three cybercrime "perpetrator" countries in the annual ranking published by the U.S.-based Internet Crime Complaint Center. [57] In 2007, the government established the Directorate for Cybersecurity to respond to criminal activities related to the internet, granting it a budget of 1.2 billion naira (US$7.8 million).[58] The directorate has since ceased to exist, but in August 2010 the government approved the formation of a Computer Crime Prosecution Unit, to be supervised by the Justice Ministry's Public Prosecution Department.[59] Cyberattacks are not prevalent, though the website of the National Assembly was hacked on October 1, 2010 by activists who posted remarks criticizing the ruling elite for poor governance and

[53] *A Bill For An Act To Provide For The Establishment Of The Cyber Security And Information Protection Agency Charged With The Responsibility To Secure Computer Systems And Networks And Liaison With The Relevant Law Enforcement Agency For The Enforcement Of Cyber Crimes Laws, And For Related Matters*, Nigerian National Assembly document (HB. 154), 2010.

[54] *A Bill For An Act To Provide For The Registration Of Mobile Telephone Line For Security Reasons And For Matters Related Thereto*, Nigerian National Assembly documents (HB. 116), 2010.

[55] *A Bill For An Act To Provide For The Prohibition Of Electronic Fraud In All Electronic Transactions In Nigeria And For Other Related Matters*, Nigerian National Assembly documents (SB. 185), 2010.

[56] Nigerian Communications Commission (NCC) and National Identity Management Commission (NIMC), *Design, Development and Delivery of SIM Card Registration Solution* (Abuja: NCC and NIMC, June 15, 2009), http://www.ncc.gov.ng/Headlines/SIM_Registration_RFP.pdf.

[57] National White Collar Crime Center and Federal Bureau of Investigation, *Internet Crime Report 2006* (Washington, DC: Internet Crime Complaint Center, 2007), http://www.ic3.gov/media/annualreport/2006_ic3report.pdf.

[58] Shina Badaru, "FG Okays N 1.2 Billion for Cybersecurity Directorate," *This Day*, June 4, 2007, available at http://www.cipaco.org/spip.php?article1272; Hilary Okeke, "DfC Helpless as Scammers Wreck Havoc on Nigerians," *Nigeria Communications Week*, July 28, 2008, http://www.nigeriacommunicationsweek.com.ng/details.php?category=topnews&id=301.

[59] Gowon Emakpe, "FG Approves Prosecution Unit for Cybercrime," *Next*, August 19, 2010, http://www.234next.com/csp/cms/sites/Next/Home/5608571-146/fg_approves_prosecution_unit_for_cyber.csp.

wastefulness in spending significant resources on celebrations of Nigeria's fifty years of independence.[60]

[60] "Protest Against Wastage At 'Nigeria At 50' Anniversary: Hackers Hijack National Assembly Website," Sahara Reporters, October 2, 2010, http://www.saharareporters.com/news-page/protest-against-wastage-nigeria-50-anniversary-hackers-hijack-national-assembly-website.

PAKISTAN

	2009	2011
INTERNET FREEDOM STATUS	n/a	Partly Free
Obstacles to Access	n/a	16
Limits on Content	n/a	17
Violations of User Rights	n/a	22
Total	n/a	55

POPULATION: 184.8 million
INTERNET PENETRATION: 11 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

With the explosion of mobile-phone use and the gradual spread of broadband internet in Pakistan, access to information and communication technologies (ICTs) has increased, as have citizen journalism and online activism. In response, over the past three to four years—under both military rule and an ostensibly democratic civilian government—the authorities have adopted various measures to exert some control over cyberspace and the sharing of information online. Although the authorities often frame new restrictions as necessary for national security, the war on terror, or protection against blasphemous content, research has revealed that in many cases, hidden under such justifications is an ulterior motive that is political.

In the early 1990s, text-based internet was introduced to the country and the first e-mail service provider in Pakistan, ImranNet,[1] was established. The spread of e-mail and digital technologies began to expand with the initiation of the Sustainable Development Networking Programme (SDNP) in December 1992.[2] With financial assistance from the United Nations Development Programme (UNDP),[3] SDNP succeeded in enhancing computer literacy and providing dial-up internet and e-mail services to urban centers across

[1] "Brief History of IMRAN.PK, Internet Email in Pakistan," http://www.imran.com/imran.pk.html, accessed January 14, 2011.
[2] "Project Document for Sustainable Development Networking: Pakistan," Sustainable Networking Development Programme (SDNP), http://www.sdnp.undp.org/countries/as/pk/pkpdoc.html, accessed January 14, 2011.
[3] "SDNP Pakistan: Success in Networking for Development," Sustainable Networking Development Programme (SDNP), http://www.sdnp.undp.org/stories/pakistan.html.

the country[4] from five nodes based in Islamabad, Karachi, Lahore, Quetta and Peshawar.[5] In 1994-95, Digicom, an entrepreneurial Internet venture, launched the first internet service access point in Karachi.[6] This heralded the beginning of the internet industry in Pakistan. By 2002, the then-Minister of Science and Telecom and his team brought more than 800[7] cities online across the country via dial-up connections. Internet and mobile-phone penetration spread further with the deregulation of the telecom sector, though a large urban-rural divide persists.[8]

As of 2009, the number of internet users stood at around 20.4 million [9] and there were about one million broadband users as of mid-2010.[10] Mobile-phone penetration is greater. According official figures released in December 2010, there were more than 100 million mobile-phone subscribers[11] with 7 mobile companies[12], and teledensity including fixed telephone lines, wireless and mobile phones reached 65. percent of the population.[13]

OBSTACLES TO ACCESS

According to International Telecommunications Union (ITU) statistics, the penetration of internet in Pakistan was slightly over 10 percent in 2009.[14] By contrast, the penetration of mobile phones stood at 61.7 percent by the end of 2010.[15] Factors such as poor infrastructure, high costs, low literacy, difficult economic conditions, age, and culture are

[4] "SDNP Pakistan's effective use of dial-up UUCP technology to promote communication in absence of connectivity," Sustainable Networking Development Programme (SDNP), http://www.sdnp.undp.org/countries/as/pk/pkuucp.html.
[5] "SDNP Pakistan: Success in Networking for Development."
[6] Tariq Mustafa, "Internet Access in Pakistan: A Brief Review," Network Startup Resource Center, June 24, 1998, http://www.nsrc.org/db/lookup/report.php?id=898710351381:488973341&fromISO=PK.
[7] "ICT Profile- Pakistan," Asia-Pacific Development Information Programme, http://www.apdip.net/projects/dig-rev/info/pk/.
[8] Ministry of Information Technology, "De-Regulation Policy for the Telecommunication Sector," Government of Pakistan, July 2003, http://www.pakboi.gov.pk/pdf/Derregulation%20Policy.pdf.
[9] International Telecommunications Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False, accessed March 4, 2011.
[10] Pakistan Telecommunication Authority, "Telecom Indicators—Broadband Subscribers by Technology," http://www.pta.gov.pk/index.php?option=com_content&view=article&id=269:telecom-indicators&catid=124:industry-report&Itemid=599, accessed January 14, 2010.
[11] "Mobile Phone Users Cross 99m Mark," *The Express Tribune*, August 17, 2010, http://tribune.com.pk/story/40007/mobile-phone-users-cross-99m-mark/.
[12] Pakistan Telecommunications Authority, "List of Mobile Operators," http://www.pta.gov.pk/index.php?option=com_content&task=view&id=850&Itemid=625, accessed February 24, 2011.
[13] Pakistan Telecommunication Authority, "Telecom Indicators," http://www.pta.gov.pk/index.php?option=com_content&view=article&id=269:telecom-indicators&catid=124:industry-report&Itemid=599, accessed February 24, 2011.
[14] ITU, "ICT Statistics 2009—Internet."
[15] Pakistan Telecommunication Authority, "Telecom Indicators—Annual Cellular Mobile Teledensity," http://www.pta.gov.pk/index.php?option=com_content&view=article&id=269:telecom-indicators&catid=124:industry-report&Itemid=599, accessed January 14, 2011.

some of the constraints that have particularly limited the development and proliferation of the internet in Pakistan.[16] High prices, poor copper wire infrastructure, and inadequate monitoring of service quality by the government regulator have further limited the expansion of broadband internet penetration.[17] Even though the prices for internet use have fallen considerably in the last few years,[18] access remains out of the reach of the majority of people in Pakistan. Most users in Pakistan access the internet either at their workplace or as students at universities and colleges. Cybercafes provide some internet service but are limited to major cities.

In June 2010**,** the minister in charge of information technologies reported a growth by 150 percent in broadband access since 2008;[19] however, these figures can be misleading given the poor quality of the connections. High quality broadband services remain concentrated in large cities like Karachi, Lahore, and Islamabad. Wireless service providers using WiMAX and EVDO along with mobile operators Mobilink, Ufone, Telenor, Warid, and Zong have also been struggling to attract consumers due to high prices and poor performance and coverage. Pakistan does not yet have a third generation (3G) network, which is also a hindrance for the spread of broadband internet and other wireless services.[20] Remote areas of the country have no access to broadband, and are left with only a slow, intermittent dial-up connection, rendering any meaningful online activities very difficult.[21] This situation is particularly challenging for students in rural areas who seek to study via distance learning, but are then deprived of multimedia lectures and tutorials. In addition, most of the areas in the conflict-stricken Khyber Pakhtunkhwa (formerly Northwest Frontier Province) and the Federally Administered Tribal Areas (FATA) are without internet access at all.

Promoting access to the internet for the masses has not been a development priority for the government, and few resources have been allocated for this purpose. The only example of such an investment has been the establishment of 365 Rabta Ghar[22] (public telecenters in rural areas) by the PTA as a pilot project; however, little information is

[16] A. Khan, *Gender Dimensions of the Information Communication Technologies for Development* (Karlstad: University of Karlstad Press, 2009).
[17] Muhammad Jamil Bhatti, "Broadband Faces Obstacles in Pakistan," Ohmy News, December 20, 2006, http://english.ohmynews.com/articleview/article_view.asp?at_code=381272.
[18] Ahmad Sajjad, "Pakistan Broadband Free Fall," blog post, Ahmad Sajjad Blog, March 3, 2008, http://sajjadzaidi.com/2008/mar/pakistan_broadband_free_fall/.
[19] Pakistan Telecommunications Authority, "2009-2010 Annual Report," http://www.pta.gov.pk/annual-reports/pta_ann_rep_2010.pdf, accessed January 14, 2011.
[20] "3G Mobile Phones but no 3G Networks in Pakistan," blog post, Mobile Phones Blog, June 16, 2010, http://www.best-mobiles.com/3g-mobile-phones-but-no-3g-networks-in-pakistan/.
[21] Pakistan Ministry of Information Technology, "Broadband Penetration in Pakistan: Current Scenario and Future Prospects," http://202.83.164.26/wps/wcm/connect/9a156580487ff5f7adaefd84e866145a/MoITStudyonBroadbandPenetration.pdf?MOD=AJPERES&CACHEID=9a156580487ff5f7adaefd84e866145a&CACHEID=9a156580487ff5f7adaefd84e866145a&CACHEID=9a156580487ff5f7adaefd84e866145a, accessed January 14, 2011.
[22] Babar Bhatti, "Rabta Ghar Updates—PTA Press Release," Telecom PK, January 7, 2009, http://telecompk.net/2009/01/07/rabta-ghar-updates/.

available on their current status or impact. Financial incentives, cultural traditions, language barriers, and most importantly, the lack of a robust telecommunications infrastructure, also weigh against great expansion of internet connectivity.

In recent years, the Pakistani authorities, either via government order or court decisions, have on several occasions blocked access to various Web 2.0 applications, such as the video-sharing website YouTube, the photo-sharing application Flickr, and the social-networking tool Facebook.[23] Such blocks are often carried out under the rubric of restricting access to "blasphemous" content; however, further research into the individual incidents has found that the restrictions consistently corresponded to circumstances suggesting politically-motivated censorship.[24] The blanket shut downs have affected a large number of users. For example, the most recent incident was a ban on Facebook that occurred on May 19, 2010 (see details below). At the time, there were approximately 2.5 million Facebook users[25] in Pakistan, and according to Alexa.com, it was the country's third most popular website.[26]

The first incident of blocking occurred at the end of February 2006 when the Pakistan Telecommunication Authority (PTA) issued instructions to all internet-service providers (ISPs) in Pakistan to block any website displaying the controversial cartoon images of the prophet Muhammad that had been published in a Danish newspaper. The block particularly focused on Google and Blogspot, a blog-hosting service.[27] The ban continued for approximately two months.[28] More recently, upon orders from the Lahore High Court, the PTA, using the pretext of limiting the circulation of blasphemous content, instituted an extensive blockage of internet content from May 19 to 31, 2010.[29] The heightened restrictions were in response to the creation of a "Everybody Draw Mohammed Day" contest on Facebook and a legal appeal initiated by a relatively unknown organization called the Islamic Lawyers Movement. The ban resulted in the blocking of 10,548 websites and critical information sources like YouTube, Flickr, the user-generated online encyclopedia Wikipedia, and more.[30] Mobile-phone providers also halted Blackberry services, at first completely, but then only web-browsing functions.[31] The blocking was widely criticized by

[23] "Pakistan Blocks Access to Youtube in Internet Crackdown," British Broadcasting Corporation (BBC), May 20, 2010, http://www.bbc.co.uk/news/10130195.
[24] "How Come Content Against Salman Taseer can be Termed as 'Blasphemous'?" Bytes for All Pakistan ICT Policy Monitor Network, March 1, 2009, http://pakistanictpolicy.bytesforall.net/?q=node/160.
[25] http://www.checkfacebook.com/.
[26] http://www.alexa.com/topsites/countries/PK.
[27] Jefferson Morley, "Pakistan's Blog Blockade," blog post, *Washington Post* Blogs, March 8, 2006, http://blog.washingtonpost.com/worldopinionroundup/2006/03/pakistans_blog_blockade.html.
[28] "PTA Unblocks Blogspot," Teeth Maestro, May 3, 2006, http://teeth.com.pk/blog/2006/05/03/pta-unblocks-blogspot.
[29] Waqar Hussain, "Pakistan Blocks Facebook Over Mohammed Cartoon," Agence France-Presse (AFP), May 19, 2010, http://www.google.com/hostednews/afp/article/ALeqM5iqKZNUdJFQ6c8ctdkUW0C-vktIEA.
[30] "The Shameful Saga of the Internet Ban in Pakistan," Association for Progressive Communication (APC), July 22, 2010, http://www.apc.org/en/node/10786/.
[31] Aamir Attaa, "Blackberry Services Go Offline in Pakistan," Pro Pakistani, May 20, 2010, http://propakistani.pk/2010/05/20/blackberry-services-go-offline-in-pakistan/; Aamir Attaa, "Blackberry Services Yet to be

civil society circles, particularly given the collateral damage caused, whereby all users of these particular applications were affected. Responding to public protests, the blanket blocks were generally temporary, and as of the end of 2010, most of these services were available, though the authorities appeared to shift their efforts to blocking individual YouTube videos or Facebook pages instead (see Limits on Content). The exception was access to applications such as Facebook and Twitter via Blackberry devices, which remained restricted throughout 2010, though a range of tips for circumventing the blockage circulated online.[32]

As of December 2010, there were 50 operational ISPs[33] throughout Pakistan, along with 10 broadband service providers and 2 HFC Operators providing broadband internet. For its backbone, Pakistan is connected via the Pakistan Internet Exchange (PIE) with SEA-ME-WE 3 and 4, along with backup bandwidth provided by Trans-World Associates (TWA).[34] The current total internet bandwidth landing in Pakistan is 105,000 Mbits.[35] The licensing division of the PTA[36] is responsible for licensing telecom service providers including ISPs and mobile-phone providers; cybercafes do not require a license to operate. The process for obtaining a license for an ISP or mobile-phone provider routinely involves long bureaucratic processes and payment of hefty licensing fees. Since there is no regulatory agency to issue licenses, opening a cybercafe is relatively easy.[37]

The PTA is the primary regulatory body overseeing internet and mobile-phone services. The Prime Minister appoints the chairman and members of the PTA, and the body reports to the Ministry of Information Technology and Telecommunication.[38] Industry representatives, civil society groups, and independent experts have serious reservations about its openness and independence as a regulatory body.

Fully Restored," Pro Pakistani, June 4, 2010, http://propakistani.pk/2010/06/04/blackberry-services-yet-to-be-fully-restored/.

[32] Omair Zeeshan, "Getting Around the Blackberry Browsing Quagmire," *Express Tribune,* January 7, 2011, http://tribune.com.pk/story/97391/getting-around-the-blackberry-browsing-quagmire/; "Blackberry users in Pakistan can Migrate to Enterprise Service for Unrestricted Use," blog post, Teeth Maestro, January 23, 2011, http://teeth.com.pk/blog/2011/01/23/blackberry-users-in-pakistan-need-to-migrate-to-enterprise-service-for-unrestricted-use.

[33] Internet Service Providers Association of Pakistan (ISPAK) www.ispak.pk.

[34] "Cable and Wireless Worldwide Wins New Contract from Transworld Associates for International Data Services," Cable and Wireless Worldwide, July 21, 2010, http://www..cw.com/cable-wireless-worldwide-wins-new-contract-from-transworld-associates.

[35] Internet Service Providers Association of Pakistan (ISPAK) www.ispak.pk, accessed January 5, 2010.

[36] Pakistan Telecommunications Authority, "Functions and Responsibilities," December 24, 2004, http://www.pta.gov.pk/index.php?option=com_content&task=view&id=359&Itemid=325.

[37] Sehrish Wasif, "Dens of Sleaze," *Express Tribune*, July 22, 2010, http://tribune.com.pk/story/29455/dens-of-sleaze/.

[38] Pakistan Telecommunications Authority, "Pakistan Telecommunication (Re-organization) Act, 1996," Chapter II, Page No. 6, http://www.pta.gov.pk/media/telecom_act_170510.pdf, accessed January 14, 2011.

LIMITS ON CONTENT

Since January 2003, the government of Pakistan has taken steps to censor some online content, though the system for doing so is not particularly sophisticated.[39] The authorities primarily rely on a blacklist of URLs that are blocked at both the PIE level and by individual ISPs. According to testing conducted by the Open Net Initiative in 2006 and 2008, censorship efforts focused symbolically on pornography and websites related to religious conversion, with some restrictions being inconsistent across different ISPs. More comprehensively blocked is content perceived as anti-military, blasphemous, or anti-state, while the most systematically censored is information disseminated by Balochi and Sindhi political dissidents.[40] For example, the website of the Washington-based World Sindhi Institute[41] and the website Lal-Masjid[42] are blocked. In November 2010, the authorities blocked *The Baloch Hal,* the first English language news website focused on Baluchistan, approximately one year after its launch.[43] The authorities have cited Section 99 of the penal code, which allows the government to restrict information that might be prejudicial to the national interest,[44] to justify their blocking.

Despite such limitations, Pakistanis have relatively open access to international news organizations and other independent media, as well as a range of websites representing Pakistani political parties, local civil society groups, and international human rights organizations.[45]

However, a confidential document that the PTA submitted to the Lahore High Court in June 2010[46] and that was later obtained by activists cites a series of policy guidelines that point to government plans to expand content filtering.[47] In this document, the Ministry of IT (MIT) calls for the establishment of a system whereby an opaque Inter-Ministerial Committee for the Evaluation of Websites receives complaints from the public, the ministry, or the PTA, evaluates whether they should be blocked, and if it finds that they should be, issues a directive to the PTA for blocking either the IP address or the URL of the relevant site. The document also includes a list of vaguely worded categories of information

[39] "Country Profile—Pakistan," OpenNet Initiative, December 26, 2010, http://opennet.net/research/profiles/pakistan.
[40] Pakistan Telecommunications Authority, "Letter to All ISP/DSL Operators Regarding Blocking of Websites Access," April 25, 2006, http://pakistan451.files.wordpress.com/2006/04/PTA%20-%20Blocking%20of%20website%2025-4-06.pdf.
[41] World Sindhi Institute: http://www.worldsindhi.org/ blocked in Pakistan.
[42] "Lal Masjid issue and its Blocked Website," Teeth Maestro, April 12, 2007, http://teeth.com.pk/blog/2007/04/12/lal-masjid-issue-and-its-blocked-website.
[43] "The Baloch Hal Banned," *Baloch Hal,* November 9, 2010, http://www.thebalochhal.com/2010/11/the-baloch-hal-banned/.
[44] Pakistan Criminal Procedure Code, 1898, http://www.intermedia.org.pk/mrc/medialawdocs/CriminalProcedureCode.pdf, accessed January 14, 2011.
[45] "Country Profile—Pakistan."
[46] Ministry of Information Technology, "Policy Guidelines for Effective Monitoring and Control of Blasphemous/Offensive Content Over Internet in Pakistan," June 2010, https://boxcrack.net/boxcrack/assets/docs/Pakistan.pdf.
[47] Confidential Pakistani document reveals plans for stricter control of the internet and freedom of expression http://www.apc.org/en/news/confidential-pakistani-document-reveals-plans-stri.

considered "unsuitable," including but not limited to: "information pertaining to any objectionable content," and websites that "bring contempt to the country or its people," websites that "undermine Islam or ridicule, disparage, or attack any religion," websites that bring "contempt of the defense forces, police, air force or any other institution of government," and websites that contain "propaganda in favor of any foreign state having bearing on any point of disputes or against any friendly foreign state."[48] If implemented, these policy guidelines would significantly increase restrictions on the free flow of information over the internet.

Indeed, a September 2010 submission by the MIT to the Lahore High Court cited that the committee had begun functioning and was comprised of representatives from the MIT, Ministry of Religious Affairs, Ministry of Interior, security agencies, and the PTA, among others. According to the document, by September 2010, "more than 12,000 blasphemous and anti state/social websites have been blocked from access through the directives of the committee."[49] Specifically during August-September 2010, over 247 URLs were reportedly blocked, mostly related to an incident of a U.S.-based pastor initiating a campaign to burn copies of the Quran. A list of the banned URLs attached to the submission included web pages from international news outlets like the *New York Times* or the Cable News Network (CNN), blog postings critical of Islam, mostly based in the United States, and dozens of links to YouTube videos or Facebook groups.[50] The submission also referenced growing communication between the Pakistani authorities and administrators for websites such as Facebook and YouTube in order to prompt rapid removal of controversial content, such as the "International burn a Quran day" Facebook group.[51] No further details related to the committee's scope of work or the criteria used to inform blocking decisions have been made public, however.

Although the professed goal of the government is to limit access to pornographic materials, extremist groups, and anti-state activists, also targeted is certain information perceived as damaging to the image of the military or top politicians. In some incidents, such as the circulation of videos of a member of the armed forces being involved in land grabs,[52] or the President telling members of the audience to shut up in the middle of a public

[48] Ministry of Information Technology, "Policy Guidelines for Effective Monitoring and Control of Blasphemous/Offensive Content Over Internet in Pakistan."
[49] Ministry of Information and Technology, "Mohammad and Ahmad vs. GOP etc. in the Lahore High Court, Lahore," Government of Pakistan, September 14, 2010, http://pakistanictpolicy.bytesforall.net/files/PTA%20Response%20to%20LHC.pdf.
[50] Pakistan Telecommunication Authority (PTA), "Blocking of Websites Having Blasphemous Content," Government of Pakistan, June 25, 2010, http://pakistanictpolicy.bytesforall.net/files/Blocked-monitored-websites.pdf.
[51] Ministry of Information and Technology, "Mohammad and Ahmad vs. GOP etc. in the Lahore High Court, Lahore."
[52] Shahzad Ahmad, "Internet Censorship in Pakistan: Naval Chief Misuing His Powers," Association for Progressive Communications (APC), August 18, 2008, http://www.apc.org/en/blog/freedom/asiapacific/internet-censorship-pakistan-naval-chief-misusing-.

speech,[53] the government has blocked specific URLs; error messages seen by users refer to the censored content as "blasphemous," or that the "site is restricted," although it was apparently blocked for political reasons. By contrast, Facebook and Twitter postings by militant Islamic groups such as Hizbut al-Tahrir, including comments inciting violence against the Ahmedi religious minority, have been allowed to circulate with few restrictions.[54]

Most online commentators exercise a degree of self-censorship when writing on topics such as religion, blasphemy, separatist movements, or human rights protection for women and homosexuals, given the sensitivity of both the government and non-state actors to these subjects. There were few reports of authorities contacting bloggers to remove specific content or requiring moderators on discussion forums to delete certain messages.

A wide variety of government agencies are involved in online content censorship, but the PTA is the main body overseeing such restrictions. There are no published or known guidelines as to how or why some content is blocked, or what mechanisms may be available for challenging censorship decisions.

The relationship between citizen journalism and traditional media is mutually reinforcing, particularly with respect to a number of daring, investigative bloggers and the circulation of online videos. For example, in August 2010, a YouTube video was posted exposing the brutal killing of two brothers in the presence of senior police officers.[55] Following the video's circulation, several satellite television stations aired the story as well. This prompted the Supreme Court of Pakistan to initiate a high level inquiry into the killings. In another incident from May 2010, a mobile-phone video showing police humiliating and torturing a woman who approached a police station in Faisalabad to report a theft was posted on YouTube;[56] it too led to departmental inquiries and punishment of the perpetrators.[57] In September 2010, a mobile-phone video appeared online showing Pakistani soldiers arbitrarily killing six civilians as part of an anti-Taliban offensive in Swat valley. The

[53] "When Zardari 'Shut Up' an Inattentive Audience," *Indian Express,* February 10, 2010, http://www.indianexpress.com/news/when-zardari-shut-up-an-inattentive-audien/578139/.

[54] Issam Ahmed, "Newest Friends on Facebook? Pakistan Militants," *Christian Science Monitor,* July 8, 2010, http://www.csmonitor.com/World/Asia-South-Central/2010/0708/Newest-friends-on-Facebook-Pakistan-militants.

[55] Mob kills two young brothers in Sialkot: http://www.youtube.com/watch?v=76M42nh6nJ0&feature=related and http://www.youtube.com/watch?v=I0bC_ZAV5aU; "Two Innocent Brothers Killed in Sialkot Live," PK Mirror, August 21, 2010, http://www.pkmirror.com/2010/08/21/two-innocent-brothers-killed-in-sialkot-live/.

[56] Faisalabad Police tortures woman on filing theft complaint: http://www.youtube.com/watch?v=IjizdtPDrio&feature=related.

[57] Mohhamed Saleem, "Footages Revive Old Case: Woman's Torture Brings Police in the Dock," *Dawn*, May 3, 2010, http://news.dawn.com/wps/wcm/connect/dawn-content-library/dawn/the-newspaper/national/footages-revive-old-case-womans-torture-brings-police-in-the-dock-350; However, later on they were reinstated. Supreme Court also took suo moto notice and issued orders to arrest the police officials involved in the woman torture case: "SC Orders Arrest of Cops Involved in Torture," *The Express Tribune*, May 3, 2010, http://tribune.com.pk/story/10448/cj-takes-suo-moto-notice-on-faisalabad-torture-case/.

incident drew international attention, including debates within the United States on whether to cut funding to the Pakistani military as a result.[58]

Although many civil society groups have been able to use the internet to advance their cause, mobile phones are the predominant medium for mobilization around political and social issues. The movement from 2008 to 2010 by lawyers and others calling for the reinstatement of Supreme Court Chief Justice Iftikhar Chaudhry and greater protection of judicial independence is perhaps the most prominent example of how citizens have used social-networking websites, text-messaging, and other new media tools to successfully challenge state repression.[59] The recent floods in Pakistan have prompted many Pakistani citizens and members of the diaspora to mobilize and raise funds online on websites such as Facebook and Twitter.[60]

VIOLATIONS OF USER RIGHTS

Article 19 of the Constitution of Islamic Republic of Pakistan grants the fundamental right of freedom of speech, although it is subject to several restrictions.[61] Pakistan also became a signatory to the International Covenant on Civil and Political Rights (ICCPR)[62] in June 2010, although it added several reservations to its instrument of ratification.[63] These reservations include: (a) supremacy of the country's own constitution; (b) supremacy of Islamic ideology; and (c) self-determination on the provision of rights. In a positive development, in December 2010, a Lahore High Court judge rejected a petition requesting that the Wikileaks website be blocked to protect national security, in the process affirming the public's right to access such information. The decision raised hopes that it could potentially serve as a precedent for the future protection of citizens' right to access content online.[64]

[58] Jane Perlez, "Video Hints at Executions by Pakistanis," *New York Times*, September 29, 2010, https://www.nytimes.com/2010/09/30/world/asia/30pstan.html?pagewanted=1&_r=2; "Extrajudicial Killings by Pakistan Army," blog post, Teeth Maestro, October 3, 2010, http://teeth.com.pk/blog/2010/10/03/extra-judicial-killings-by-pakistan-army.

[59] "In Pictures: Lawyers Protest," British Broadcasting Corporation (BBC), March 12, 2007, http://news.bbc.co.uk/2/hi/in_pictures/6442747.stm.

[60] Issam Ahmed, "Pakistan Floods: How New Networks of Pakistanis are Mobilizing to Help," *Christian Science Monitor,* August 19, 2010, http://www.csmonitor.com/World/Asia-South-Central/2010/0819/Pakistan-floods-How-new-networks-of-Pakistanis-are-mobilizing-to-help.

[61] The Constitution of Pakistan and Fundamental Rights http://www.sdpi.org/know_your_rights/know%20you%20rights/The%20Constitution%20of%20Pakistan.htm.

[62] "President Signs Convention on Civil, Political Rights," Daily Times, June 4, 2010, http://www.dailytimes.com.pk/default.asp?page=2010\06\04\story_4-6-2010_pg7_18.

[63] Maheen Gul-Malik, "ICCPR and the Sialkot Incident," Daily Times, September 9, 2010, http://www.dailytimes.com.pk/default.asp?page=2010\09\09\story_9-9-2010_pg3_2.

[64] "Wikileaks Exposing People, not Damaging Nation," *Dawn*, December 11, 2010, http://www.dawn.com/2010/12/11/wikileaks-exposing-people-not-damaging-nation-lhc.html.

Several pieces of legislation are used to restrict freedom of expression, including online. In 2008, former president Pervez Musharraf introduced a draconian Prevention of Electronic Crimes Ordinance (PECO).[65] The ordinance called for long prison terms for offenses involving vaguely worded terms like "lewd" and "immoral," and declared as cyber crimes actions such as sending unsolicited text-messages and circulating photos without the permission of the person who was photographed. The ordinance was widely viewed as an effort to curb the use of digital media in organizing protests or circulating criticism of Musharraf.[66] The regulation lapsed in 2009, but was later tabled before the national assembly for approval to reactivate it. However, in November 2009, the Prime Minister returned it to the National Assembly's Standing Committee on Information Technology for further consultation and development of a new draft. In doing so, he cited its restrictive approach to free expression as the reason.[67] As of December 2010, the bill was pending and a new draft was still awaited.

Section 124 of the Pakistan Penal Code (PPC) on Sedition is extremely broadly worded, and the 2004 Defamation Act allows for imprisonment of up to five years, though neither is frequently used to punish journalists and has yet to be used to punish online speech.[68] Rather, another section of the penal code, Section 295(c), which addresses blasphemy, was used by police in 2010 to initiate proceedings against Facebook founder Mark Zuckerberg after a user of the social-networking tool created a group hosting a competition to draw the prophet Muhammad, a task considered offensive by many Muslims.[69] The maximum punishment under the law is life imprisonment or the death penalty. Following a wave of jokes about the president that circulated over e-mail, in July 2009 the government announced that several agencies had been tasked with tracing electronically transmitted jokes, and that offenders could face a 14-year prison sentence.[70] Despite such threats and the harsh legal environment, there were no Pakistani bloggers or activists imprisoned for online activities as of the end of 2010.

---

[65] "President Promulgates Ordinance to Prevent Electronic Crimes," Associated Press of Pakistan (APP), November 6, 2007, http://www.app.com.pk/en_/index.php?option=com_content&task=view&id=58277&Itemid=1.

[66] Irfan Ahmed, "New Cyber Law in Pakistan Restricts Free Speech," OneWorld South Asia, January 24, 2008, http://southasia.oneworld.net/Article/new-cyber-law-in-pakistan-restricts-free-speech.

[67] Khawar Ghumman, "Government Fails to Form Body on Electronic Crimes Bill," *Dawn*, January 6, 2010, http://www.dawn.com/wps/wcm/connect/dawn-content-library/dawn/the-newspaper/national/govt-fails-to-form-body-on-electronic-crime-bill-610.

[68] "PPC Section 124-Sedition**:** Whoever by words, either spoken or written, or by signs, or by visible representation, or otherwise, brings or attempts to bring into hatred or contempt, or excites or attempts to excite disaffection towards, the Federal or Provincial Government established by law shall be punished with imprisonment for life to which fine may be added, or with imprisonment which may extend to three years, to which fine may be added, or with fine." http://www.pakistani.org/pakistan/legislation/1860/actXLVof1860.html; Karin Deutsch Karlekar, ed., "Pakistan," in *Freedom of the Press 2010* (New York: Freedom House, 2010), http://www.freedomhouse.org/template.cfm?page=251&year=2010.

[69] Maija Palmer, "Facebook Founder Faces Pakistan Probe," *Financial Times*, June 17, 2010, http://www.ft.com/cms/s/0/3aaf867e-7a42-11df-aa69-00144feabdc0.html.

[70] "SMS Joke on Zardari May Land you in Pak Jail," *NDTV*, July 20, 2009, http://www.ndtv.com/news/world/sms_joke_on_zardari_may_land_you_in_pak_jail.php; Karlekar, ed., "Pakistan."

Fear of government surveillance is not a significant concern among most bloggers and online activists in Pakistan, with the exception of individuals in Baluchistan. Nevertheless, the Pakistani authorities and particularly intelligence agencies have some monitoring capacity. Before providing services, ISPs, telecom companies, and SIM card vendors are required to verify the National Identity Card details of prospective customers and to authenticate them with the National Database Registration Authority.[71] Although the Electronic Crimes ordinance expired in 2009, ISPs and telecom companies were reported to be continuing to keep logs of customer communications and convey them to security agencies as needed under directives from the PTA. In recent years, provincial authorities have pressured the central government to grant greater surveillance powers and location tracking ability to local police as part of efforts to curb terrorism and violent crime.[72] As of the end of 2010, it was unclear how much the authority had been broadened. According to some reports, the PIE positioned at the international internet gateway has the capability to monitor all incoming and outgoing traffic, as well as store all e-mails. In addition, Pakistan is reported to be a customer of Narus, a U.S.-based firm known for designing technology that allows for monitoring of traffic flows, as well as deep-packet inspection of internet communications.[73]

Although Pakistan is one of the most dangerous environments for traditional journalists, with at least 12 being murdered in 2009 and 2010,[74] no bloggers or online activists have been killed to date. However, during the internet crackdown that occurred in May 2010, there were several incidents of non-state actors, particularly Islamic extremists, attacking or threatening bloggers and others who were advocating against the blocking of online resources. In one instance, a mob attacked[75] a press conference[76] organized at the Karachi Press Club, though the club's personnel were able to disperse the tensions. During

[71] National Database Registration Authority (NADRA), www.nadra.gov.pk ; "Verification of CNICs: Nadra Signs Contract with Three Cell Phone Companies," NADRA, July 29, 2009, http://www.nadra.gov.pk/index.php?option=com_content&view=article&id=111:verification-of-cnics-nadra-signs-contract-with-three-cell-phone-companies&catid=10:news-a-updates&Itemid=20; Bilal Sarwari, "SIM Activation New Procedure," Pak Telecom, September 3, 2010, http://www.paktelecom.net/pakistan-telecom-news/pta-pakistan-telecom-news/sim-activation-new-procedure/.

[72] Masroor Afzal Pasha, "Sindh Police To Get Mobile Tracking Technology," *Daily Times,* October 29, 2010, http://www.dailytimes.com.pk/default.asp?page=2010\10\29\story_29-10-2010_pg7_18; "Punjab Police Lack Facility of 'Phone Locator', PA Told," *The News,* January 12, 2011, http://www.thenews.com.pk/TodaysPrintDetail.aspx?ID=25244&Cat=2&dt=1/14/2011.

[73] Timothy Carr, "One U.S. Correspondent's Role in Egypt's Brutal Crackdown," Huffington Post, January 28, 2011, http://www.huffingtonpost.com/timothy-karr/one-us-corporations-role-_b_815281.html; "Narus: Security Through Surveillance," Berkman Center for Internet and Society at Harvard University, November 11, 2008, http://blogs.law.harvard.edu/surveillance/2008/11/11/narus-security-through-surveillance/.

[74] "Journalists Killed in Pakistan Since 1992," Committee to Protect Journalists (CPJ), http://cpj.org/killed/asia/pakistan/, accessed February 24, 2011.

[75] Farieha Aziz, "Critics of Facebook Ban Face Nasty Battle," *Newsline Magazine*, May 21, 2010, http://www.newslinemagazine.com/2010/05/critics-of-facebook-ban-face-nasty-battle/.

[76] Samia Saleem, "Conference on Internet Censorship Ends on Sour Note," *The Express Tribune*, May 20, 2010, http://tribune.com.pk/story/14763/conference-on-internet-censorship-ends-on-sour-note/.

the same period, several free expression activists and bloggers received anonymous death threats. Most such messages were sent via text message from untraceable, unregistered mobile-phone connections, usually originating from the tribal areas of the country, and several had very specific details related to the individuals' profile or recent activities. Similarly, as some militant Islamic groups consider cybercafes to be sites of moral degradation, they have initiated attacks and bombings of such access points. Most attacks have occurred in Khyber Pakhtunkhwa Province and FATA, but in July 2010, bomb blasts also struck two cybercafes in Lahore, injuring six people.[77]

[77] Mohammad Faisal Ali, "Six Injured in Two Lahore Blasts," *Dawn*, July 18, 2010, http://www.dawn.com/wps/wcm/connect/dawn-content-library/dawn/news/pakistan/metropolitan/03-explosion-reported-in-garhi-shahu-lahore-ss-08 .

RUSSIA

	2009	2011
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access	11	12
Limits on Content	16	17
Violations of User Rights	22	23
Total	**49**	**52**

POPULATION: 141.9 million
INTERNET PENETRATION: 33 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

After the elimination of independent television channels and the tightening of press regulations in 2000–01, the internet became Russia's last relatively uncensored platform for public debate and the expression of political opinions. However, even as access conditions have improved, internet freedom has corroded. In the last two years there have been several cases of technical blocking and numerous cases of content removal. The authorities have also increasingly engaged in harassment of bloggers. At least 25 cases of blogger harassment, including 11 arrests, were registered between January 2009 and May 2010, compared with seven in 2006–08. In addition, dozens of blogs have reportedly been attacked in recent years by a hacker team called the Hell Brigade.[1]

Since the internet was first launched in Russia in 1988, the country has made significant gains in the expansion of its information infrastructure. Most Russians access the internet from their homes (94 percent of users) and workplaces (48 percent), and use of cybercafes has consequently dropped off.[2] Internet access via mobile telephones and similar devices has gained popularity since 2006, and 9.4 million people report using this method.[3] Faster and more credible than conventional media, online outlets are becoming the main

[1] Vladimir Pribylovski, "Список взломанных бригадой хелла ЖЖ-блогов" [List of LiveJournal Blogs Hacked by Hell Brigade], LJ.Rossia.org, http://lj.rossia.org/users/anticompromat/769184.html (in Russian), accessed January 2011.
[2] Public Opinion Foundation, "Новый выпуск бюллетеня 'Интернет в России, Зима 2009/2010'" [New Issue of the Bulletin 'Internet in Russia, Winter 2009/2010'], news release, March 24, 2010, http://bd.fom.ru/report/cat/smi/smi_int/int240310_pressr (in Russian).
[3] Taylor Nelson Sofres (TNS), "Аудитория мобильного интернета приблизилась к 10 млн" [Mobile Internet Audience Has Reached 10 Million], RuMetrika, November 22, 2010, http://rumetrika.rambler.ru/review/0/4578 (in Russian).

information source for a growing number of Russians, and certain websites have larger audiences than television channels.

OBSTACLES TO ACCESS

Internet and mobile-phone penetration in Russia continue to grow, and the government largely supports the dissemination of these technologies, both directly and through state-controlled internet-service providers (ISPs) that offer relatively low broadband prices. The number of internet users jumped from 1.5 million in 1999 to 46.5 million in 2010,[4] and grew by more than 13 million in the last two years, though this still leaves Russia's penetration rate at 33 percent, lower than the rates in Central European countries. The level of infrastructure differs significantly from place to place, and gaps are evident between urban and rural areas as well as between different types of cities. The worst access conditions can be found in the North Caucasus and the industrial towns of Siberia and the Far East. In 2009, broadband penetration reached approximately 31 percent of internet users, or 15.7 million households, up from 8.3 million in 2008.[5] Unlimited-plan prices in the different federal districts vary from US$10 to US$69 a month.[6] By the end of 2008, the majority of schools were connected to the internet, but connection speeds are sometimes low. Libraries have been connected less extensively. Internet cafes are present in almost every city.

Mobile-phone penetration has grown rapidly in recent years, and there were 163 subscriptions per 100 inhabitants in 2009.[7] Third-generation (3G) mobile-phone infrastructure began developing relatively late due to resistance from military officials, who claimed that the technology might weaken national security.[8] Now approximately 21 percent of mobile subscribers, mostly in the largest cities, own 3G phones, and the 3G network is expanding rapidly.

Applications like the social networking site Facebook, the Russian social networking site VKontakte, the Twitter microblogging platform, and various international blog-hosting services are freely available. The video-sharing site YouTube is currently accessible, although it has come under threat in some localities. For example, in July 2010, a court in Komsomolsk-on-Amur issued a decision instructing a local ISP to block YouTube, along

[4] *Интернет в России* [Internet in Russia] no. 31 (Autumn 2010), http://bd.fom.ru/pdf/Bulliten_31_osen_2010_short.pdf (in Russian).
[5] iKS-Consulting, "Общероссийские показатели ШПД активно растут" [Russia's Broadband Indices Grow Rapidly], RuMetrika, October 15, 2010, http://rumetrika.rambler.ru/review/0/4524 (in Russian).
[6] Alexey Sidorenko, "Russia: Mapping Broadband Internet Prices," Global Voices, March 14, 2010, http://globalvoicesonline.org/2010/03/14/russia-mapping-broadband-internet-prices/.
[7] International Telecommunication Union (ITU), "ICT Statistics 2009—Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx, accessed February 14, 2010.
[8] The frequency used by 3G had been restricted by the military as "strategic."

with four other websites, because they hosted extremist content including copies of Adolf Hitler's *Mein Kampf* and skinhead videos. The ruling was later overturned after the provider filed an appeal.[9] Also in July, a court in Ingushetia ordered local providers to ban the entire blogging platform LiveJournal because it hosted a blog deemed to promote terrorism and extremism.[10]

Five access providers—Comstar, Vimpelcom, ER-Telecom, AKADO, and the state-owned SvyazInvest—controlled more than 67 percent of the broadband market as of February 2010.[11] Regional branches of SvyazInvest account for 36 percent of subscribers, up from 27.8 percent in 2008. As at the federal level, regional dominance usually depends on political connections and the tacit approval of regional authorities. Although this situation is not the direct result of legal or economic obstacles, it nonetheless reflects an element of corruption that is widespread in the telecommunications sector and other parts of the Russian economy.

Three leading operators—MTS, Vimpelcom, and MegaFon—hold 83 percent of the mobile-phone market.[12] While formally independent, each of these firms has indirect ties to the government. According to independent analyst Vadim Gorshkov, MegaFon is connected with former minister of telecommunications Leonid Reyman, and MTS is linked to the Moscow regional leadership. The information and communications technology (ICT) sector is regulated by the Federal Service for the Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor), whose director is appointed by the prime minister. Given Russia's closed political system and dominant executive branch, the appointment process is not transparent. There are no special restrictions on opening cybercafes or starting ISP businesses, but unfair competition and other such obstacles are not unusual in Russia.

LIMITS ON CONTENT

Although attempts to establish a comprehensive, centralized filtering system have been abandoned, several recent cases of blocking have been reported. In December 2009, a

[9] Alexey Sidorenko, "Russia: The First Case of YouTube Ban," Global Voices, July 30, 2010, http://globalvoicesonline.org/2010/07/30/russia-the-first-case-of-youtube-ban/.
[10] "В Ингушетии заблокировали весь ЖЖ из-за одного блога" [In Ingushetia Entire LiveJournal Blocked Because of One Blog], CNews, August 5, 2010, http://www.cnews.ru/news/line/index.shtml?2010/08/05/403880 (in Russian).
[11] Advanced Communications and Media, "Russian Residential Broadband Data, February 2010," news release, April 23, 2010, http://www.acm-consulting.com/news-and-data/data-downloads/cat_view/16-broadband.html?orderby=dmdate_published.
[12] J'son & Partners Consulting, "Информационный бюллетень: Сотовая Связь в России, Июнь 2009" [Information Bulletin: Mobile Communications in Russia, June 2009], http://www.json.ru/files/news/Cellular_Market_Watch_June_09_RUS.pdf (in Russian), accessed May 2010.

number of ISPs blocked access to the radical Islamist website Kavkaz Center.[13] At almost the same time, the wireless provider Yota blocked several opposition sites.[14] The practice of exerting pressure on service providers and content producers by telephone has become increasingly common. Police and representatives of the prosecutor's office call the owners and shareholders of websites, and anyone else in a position to remove unwanted material and ensure that the problem does not come up again. Such pressure encourages self-censorship, and most providers do not wait for court orders to remove targeted materials. As a result, there has been a massive exodus of opposition websites to foreign site-hosting providers, as well as a trend toward greater use of social networking sites.

Regional blocking, whereby a website is blocked in some areas but remains available elsewhere in the country, is one of the methods used by the authorities to exert more control over the internet. Apart from the YouTube incidents mentioned above (see "Obstacles to Access"), a state-controlled local provider in August 2010 blocked the independent portal *Tulksiye Pryaniki*, which had published articles that were critical of the government. In another example of the phenomenon, a regional network provider in December 2010 temporarily blocked its users from accessing the environmentalist website Ecmo.ru, allegedly because the site initiated a petition to dismiss a local mayor. Regional blocking is arguably more efficient than nationwide blocking in that it attracts less attention and affects only the most relevant audiences.[15]

Content is often removed on the grounds that it violates Russia's laws against "extremism." Providers are punished for hosting materials that are proscribed in a list on the website of the Ministry of Justice.[16] The list is updated on a monthly basis and included 748 items as of January 2011.[17] The procedure for identifying extremist materials is nontransparent, leaving ample room for politically motivated content removal.[18] There have

[13] "Воронка стала достоянием общественности, а лживые сомнения были развеяны вторым взрывом" [The Shell Hole Went Public, and Fake Doubts Were Dispersed by a Second Blow], *Norvezhskiy Lesnoy* (blog), December 2, 2009, http://nl.livejournal.com/869414.html (in Russian).

[14] "Фильтры от Yota" [Filters from Yota], *Drugoi* (blog), December 5, 2009, http://drugoi.livejournal.com/3111589.html (in Russian). The sites blocked were Kasparov.ru, Rufront.ru, Rusolidarnost.ru, Nazbol.ru, Namarsh.ru, and Newtimes.ru. Later the provider explained that there was a technical problem, although journalists at the *Moscow Times* found evidence to the contrary. See Nikolaus von Twickel, "Internet Provider Says It Blocks Sites," *Moscow Times*, December 8, 2009, http://www.themoscowtimes.com/news/article/internet-provider-says-it-blocks-sites/391080.html.

[15] "It's Not the Kremlin," *Babbage* (blog), *Economist*, August 25, 2010, http://www.economist.com/blogs/babbage/2010/08/internet_censorship_russia.

[16] Two such cases occurred in the Kirov and Khanty-Mansiisk regions. See Alexey Sidorenko, "Russia: Hosting Providers Sued for Refusal to Block Web Sites," Global Voices, May 13, 2010, http://globalvoicesonline.org/2010/05/13/russia-hosting-providers-sued-for-refusal-to-block-web-sites/; "Провайдера обязали ограничить доступ к экстремистским сайтам" [Provider Obliged to Filter Extremist Sites], Regnum, February 24, 2010, http://www.regnum.ru/news/1256707.html (in Russian).

[17] Ministry of Justice, "Федеральный список экстремистских материалов" [Federal List of Extremist Materials], http://www.minjust.ru/ru/activity/nko/fedspisok/ (in Russian), accessed May 2010.

[18] As Dmitri Solovyev's case showed, the results may vary depending on the institution where the extremism check was performed. See Alexey Sidorenko, "Russia: Prosecution Against Opposition Blogger Stopped," Global Voices, January 28, 2010, http://globalvoicesonline.org/2010/01/28/russia-prosecution-against-opposition-blogger-stopped/.

been at least three cases of site closures, two of them temporary, on the grounds that the affected sites hosted extremist materials.[19] In February 2010, the major opposition portal Grani.ru was checked for extremism, but the authorities apparently found nothing incriminating.[20]

Nonpolitical reasons for content removal have also been reported, with most involving child pornography and file-sharing services that violate copyright law. In May 2010, eight hosting providers, which together control over 30 percent of the hosting market, signed a charter designed to fight child pornography.[21] The agreement places responsibility for content with the hosting providers, calls on them to install monitoring mechanisms, and urges closer cooperation with police.[22] In June, over 5,000 websites containing sexually explicit images of minors were identified by the Friendly RuNet foundation, which works with various government agencies and ISPs; the sites were subsequently shut down.[23] With respect to copyright violations, the file-sharing site iFolder.ru was blocked by police for several days during the year, but the most prominent recent episode was the early 2010 suspension of the domain of the largest Russian file-tracker, Torrents.ru, by regional registrar Ru-Center.[24]

Russia's vibrant blogosphere includes over 7.4 million blogs, up from 3.8 million in 2008. Approximately 93 percent of Russian-language bloggers live inside the country,[25] and Moscow-based bloggers dominate the community.[26] President Dmitri Medvedev started a video blog in October 2007,[27] in January 2009 he established a LiveJournal blog,[28] and in June 2010 he opened a Twitter account.[29] Since then at least 39 regional governors have followed suit.[30] During the last year and a half, the role of the blogosphere grew significantly as it became not only the sole credible source of information—especially during disasters or

[19] The affected sites were Alleng.ru, 20marta.ru, and Stringer.ru.
[20] Alexey Sidorenko, "Russia: Media Portal Undergoes Check for Extremism," Global Voices, February 21, 2010, http://globalvoicesonline.org/2010/02/21/russia-media-portal-undergoes-check-for-extremism/.
[21] "Хостеры подписали декларацию против детской порнографии" [Hosters Signed Petition Against Child Pornography], CyberSecurity.ru, May 30, 2010, http://www.cybersecurity.ru/news/94903.html (in Russian).
[22] The text of the providers' joint declaration can be found at http://hostdeclaration.ru/ (in Russian), accessed May 2010.
[23] "За полгода в Рунете нашли пять тысяч сайтов с детской порнографией" [Within Half a Year, 5,000 Sites with Child Pornography Were Found on the Russian Internet], Lenta.ru, July 16, 2010, http://lenta.ru/news/2010/07/16/mvd/ (in Russian).
[24] Gregory Asmolov, "Russia: Closure of Torrents.ru Makes People Suspicious of .Ru Zone," Global Voices, February 26, 2010, http://globalvoicesonline.org/2010/02/26/torrents-sochi/.
[25] Yandex, *Блогосфера Рунета, Весна 2009* [Blogosphere of the Russian Internet, Spring 2009] (Moscow: Yandex, 2009), http://download.yandex.ru/company/yandex_on_blogosphere_spring_2009.pdf (in Russian).
[26] About 67 percent of the top bloggers reside in the capital. See "Территориальная ассиметрия русскоязычной блогосферы" [Territorial Asymmetry of the Russian-Language Blogosphere," *Blogosphere* (blog), November 29, 2009, http://habrahabr.ru/blogs/blogosphere/76734/ (in Russian).
[27] The Russian president's video blog is located at http://blog.kremlin.ru/.
[28] Dmitry Medvedev's LiveJournal blog is located at http://community.livejournal.com/blog_medvedev/.
[29] Yelena Osipova, "@MedvedevRussia, Are You Listening? A Story of 6 Months on Twitter," Global Voices, December 15, 2010, http://globalvoicesonline.org/2010/12/15/medvedevrussia-are-you-listening-a-story-of-6-months-on-twitter/.
[30] "Чиновники в сети" [Officials on the Net], *Vedomosti*, December 3, 2010, http://www.vedomosti.ru/special/governors-communications.shtml (in Russian).

extraordinary events like the Moscow subway bombings,[31] deadly fire in Perm,[32] and the summer 2010 wildfires[33]—but also the main platform for social mobilization. Several blog campaigns were quite successful,[34] although bloggers' actions came to nothing when attempting to address major cases involving senior officials.[35]

The blog-hosting platforms LiveJournal, LiveInternet, Blogs.mail.ru, and Ya.ru together host 76 percent of all active Russian-language blogs.[36] LiveJournal retains its leading position, although it is facing serious competition from its rivals. The Kremlin allegedly influences the blogosphere through media organizations as well as the progovernment youth movements Nashi (Ours) and Molodaya Gvardiya (Young Guard).[37] The emergence of competing propagandist websites has led to the creation of a vast amount of content that collectively dominates search results, among other effects.[38] Propagandist commentators simultaneously react to discussions of "taboo" topics, including the historical role of Soviet leader Joseph Stalin, political opposition, dissidents like Mikhail Khodorkovsky, murdered journalists, and cases of international conflict or rivalry (with countries such as Estonia, Georgia, and Ukraine, but also with the foreign policies of the United States and the European Union). Minority languages are underrepresented in Russia's blogosphere.

As social networking sites and blogging platforms have grown in importance, they have caught the attention of both the government and Kremlin-friendly business magnates, or "oligarchs." Metals magnate Alisher Usmanov owns 50 percent of SUP, the company that owns LiveJournal, as well as a 35 percent stake in Digital Sky Technologies, which owns the two most popular social networking sites in Russia and a number of others elsewhere in the

[31] Alexey Sidorenko, "Russia: Initial Coverage of the Moscow Subway Bombings," Global Voices, March 29, 2010, http://globalvoicesonline.org/2010/03/29/russia-initial-coverage-of-the-moscow-subway-bombings/.

[32] Gregory Asmolov, "Russia: Online Forum Beats Media in Covering Night Club Fire," Global Voices, December 5, 2009, http://globalvoicesonline.org/2009/12/05/russia-online-forum-beats-media-in-covering-night-club-fire/.

[33] One of the best citizen initiatives to map the wildfires and provide up-to-date information is the Russian Fires website, accessible at http://www.russian-fires.ru/.

[34] The positive outcomes included the punishment of a police officer who abused his authority, the rescue of a Russian tourist bitten by a snake in Indonesia, and the granting of a passport to opposition blogger Oleg Kozlovsky. See Alexey Sidorenko, "Russia: Blogger's Video Leads to Punishment of Policeman," Global Voices, March 9, 2010, http://globalvoicesonline.org/2010/03/09/russia-bloggers-video-leads-to-punishment-of-policeman/; Alexey Sidorenko, "Russia: Bloggers Saved Tourist's Life," Global Voices, February 4, 2010, http://globalvoicesonline.org/2010/02/04/russia-bloggers-saved-tourists-life/; Alexey Sidorenko, "Russia: Opposition Blogger Finally Gets Permission to Leave Country," Global Voices, January 29, 2010, http://globalvoicesonline.org/2010/01/29/russia-opposition-blogger-finally-gets-permission-to-leave-country/.

[35] For example, an online video in which police whistleblower Aleksey Dymovsky complained of widespread corruption led only to his own conviction for slander in March 2010, and bloggers' protests failed to persuade authorities to hold oil executive Anatoly Barkov accountable for a February 2010 automobile accident that killed two women.

[36] Yandex, *Блогосфера Рунета, Весна 2009*.

[37] The Kremlin-affiliated media organizations include the Foundation on Effective Politics, led by Gleb Pavlovsky; New Media Stars, led by Konstantin Rykov; and the Political Climate Center, led by Aleksey Chesnakov.

[38] Ksenia Veretennikova, "'Медведиахолдинг': Единая Россия решила формировать собственное медиапространство" ['Medvediaholding': United Russia Decided to Form Its Own Media Space], *Vremya*, August 21, 2008, http://www.vremya.ru/2008/152/4/210951.html (in Russian).

former Soviet Union. Mikhail Prokhorov, another billionaire oligarch, owns RosBusinessConsulting (RBC), whose hosting service is home to 19 percent of all Russian websites.[39] Vladimir Potanin owns Prof-Media, which in turn owns the search engine Rambler.ru, its news portal Lenta.ru, and other popular resources. Yuri Kovalchuk, a close friend of Prime Minister Vladimir Putin's who controls the media arm of state-owned energy giant Gazprom, recently bought RuTube, the Russian analogue of YouTube.[40] This oligarchic control over an important bloc of online media, social-networking applications, and blogging platforms has raised concerns about the Russian internet's vulnerability to political manipulation.

VIOLATIONS OF USER RIGHTS

Although the constitution grants the right of free speech, this guarantee is routinely violated, and there are no special laws protecting online modes of expression. Online journalists do not possess the same rights as traditional journalists unless they register their websites as mass media. Recent police practice has been to target online expression using Article 282 of the criminal code, which restricts "extremism." The term is vaguely defined and includes xenophobia and incitement of hatred toward a "social group."

Since January 2009, police and the prosecutor's office have launched at least 25 criminal cases against bloggers and forum commentators. While some cases were against individuals who posted clearly extremist content, others appear to be more politically motivated. The most severe and widely known sentence was that of Irek Murtazin, a Tatarstan blogger and journalist who received almost two years in prison in November 2009 for defamation. Other important cases include the August 2009 arrest of five people affiliated with the website Ufa Gubernskaya for extremism, and the May 2010 arrest of blogger Alauddin Dudko, who had worked with Ingush opposition journalist Magomed Yevloyev before his murder in 2008. Dudko was accused of possessing drugs and explosives, but his colleagues argued that the real reason behind the arrest was his online activity.[41] Similarly, in Ulyanovsk region, environmentalist blogger and activist Aleksandr Bragin was

[39] RBC Information Systems, *Годовой отчет РБК за 2008 год* [RBC Annual Report 2008] (Moscow: RBC, 2009), http://www.rbcinfosystems.ru/ir/2008.pdf (in Russian).
[40] Open Source Center, "Kremlin Allies' Expanding Control of Runet Provokes Only Limited Opposition," Office of the U.S. Director of National Intelligence, February 28, 2010, available at http://www.fas.org/irp/dni/osc/runet.pdf.
[41] "В Москве по обвинению в хранении наркотиков и взрывчатки задержан известный блогер" [Popular Blogger Detained in Moscow on Charges of Possession of Narcotics and Explosives], EuIngush, May 20, 2010, http://euingush.com/index.php?newsid=1424 (in Russian).

recently accused of a hit-and-run accident; Bragin claims that he was framed by the authorities in response to his investigative reporting.[42]

Only one blogger, Dmitri Solovyev of Kemerevo, was able to defend his name in court, ultimately securing the government's recognition that the blog post in question was not extremist.[43] The issue of responsibility for anonymous comments has been raised as well. The administrator of the site Gorodirbit.ru lost a court case in March 2010 over an anonymous comment about local authorities and had to pay a fine.[44]

While traditional journalists and activists have faced a series of murders and severe beatings in recent years, physical attacks on Russian bloggers and online activists have so far been comparatively limited. However, one recent event drew significant attention. In November 2010, Oleg Kashin, a reporter for the newspaper *Kommersant* who was also well known as a blogger, was severely beaten near his home in Moscow. His coverage of protests and political youth movements had prompted vocal responses from pro-Kremlin groups in the past, but it was not known exactly who was responsible for the attack.

It is unclear to what extent internet users in Russia are subject to extralegal surveillance of their online activities. Since 2000, all ISPs have been obliged to install the "system for operational investigative measures,"[45] or SORM-2, which gives the Federal Security Service (FSB) and police access to internet traffic. The system is analogous to the Carnivore/DCS1000 software used by the U.S. Federal Bureau of Investigation (FBI), and operates as a packet-sniffer that can analyze and log data passing through a digital network.[46] However, no known cases of SORM-2 use have been reported, and the efficiency of the system has been seriously questioned. Legislation approved in April 2007 allows government services to intercept data traffic without a warrant. Online surveillance represents much less of a threat in the major cities of Moscow and St. Petersburg than in the regions, where almost every significant blog or forum is monitored by the local police and prosecutor's office. Most of the harassment suffered by critical bloggers and other online activists in Russia occurs in the regions.

[42] Mikhail Byeliy, "'Это наезд': Эколог, получавший многочисленные угрозы, стал участником странного ДТП" ['This Is a Shakedown': Environmentalist, Having Received Numerous Threats, Became Involved in a Strange Accident], *Noviye Izvestiya*, November 30, 2010, http://www.newizv.ru/news/2010-11-30/137219/ (in Russian).

[43] Alexey Sidorenko, "Russia: Prosecution Against Opposition Blogger Stopped," Global Voices, January 28, 2010, http://globalvoicesonline.org/2010/01/28/russia-prosecution-against-opposition-blogger-stopped/.

[44] Igor Lesovskikh, "Владелец сайта доплатит за комментарий" [Owner of Website Will Pay for Comment], *Kommersant*, March 3, 2010, http://www.kommersant.ru/doc.aspx?DocsID=1330650 (in Russian).

[45] Konstantin Nikashov, "СОРМ для IP-коммуникаций: требуется новая концепция" [SORM for IP-Communications: New Concept Needed], Iksmedia.ru, December 10, 2007, http://www.iksmedia.ru/topics/analytical/effort/261924.html?__pv=1 (in Russian). For more information on SORM, see V. S. Yelagin, "СОРМ-2 история, становление, перспективы" [SORM-2 History, Formation, Prospects], Protei, http://www.sorm-li.ru/sorm2.html (in Russian), accessed March 20, 2009.

[46] B. S. Goldstein, Y. A. Kryukov, and V. I. Polyantsev, "Проблемы и Решения СОРМ-2" [Problems and Solutions of SORM-2], *Vestnik Svyazi* no. 12 (2006), http://www.protei.ru/company/pdf/publications/2007/2007-003.pdf (in Russian).

In addition to official monitoring and prosecution, critical websites face censorship in the form of unexpected "technical difficulties." For example, the sites Sineevedro.ru, Navalny.ru, and Novayagazeta.ru have been unavailable due to "technical reasons" during important civic actions. Several newspaper websites have experienced denial-of-service (DoS) attacks,[47] typically in connection with articles that could seriously influence offline events. Hacker attacks on blogs that began in 2007 continued in 2009–10, with at least 16 blogs suffering attacks in the last two years.[48] As in previous years, the blogs were ravaged and defaced.

Cybercrime is a serious problem, and roughly 9 percent of all internet attacks worldwide between July and September 2010 were carried out from Russia.[49] A number of factors contribute to this growing threat. First, many personal computers in Russia are not protected by antivirus software, leaving them vulnerable to infection and integration into "botnets"—networks of computers that are controlled remotely for malicious purposes. Second, information and instruction on how to build and develop botnets is widely accessible. Finally, punishment of cybercriminals is rare, contributing to a culture of impunity. According to some sources, many hackers for hire are willing to carry out DoS attacks for as little as €200 (US$260) per day.[50] Russian law enforcement has not actively pursued cybercriminals due to corruption and a lack of technical skills, but also because most of the attacks originating in Russia are aimed at users abroad, including in Europe and the United States.

[47] These included *Kommersant* in March 2009, *Novaya Gazeta* in January 2010, and *Vedomosti* in February 2010. See "'КоммерсантЪ' подвергся DDoS атаке" ['Kommersant' Has Undergone DDoS Attack], Xakep.ru, March 16, 2009, http://www.xakep.ru/post/47483/default.asp (in Russian); Alexey Sidorenko, "Russia: Newspaper Web Site Hacked," Global Voices, January 26, 2010, http://globalvoicesonline.org/2010/01/26/russia-newspaper-web-site-hacked/; Alexey Sidorenko, "Russia: Another Newspaper Web Site Attacked," Global Voices, February 13, 2010, http://globalvoicesonline.org/2010/02/13/russia-another-newspaper-web-site-attacked/.

[48] Pribylovski, "Список взломанных бригадой хелла ЖЖ-блогов."

[49] Akamai, *State of the Internet: 3st Quarter 2010 Report* (Cambridge, MA: Akamai, 2011), http://www.akamai.com/dl/whitepapers/Akamai_soti_apac_q310.pdf?curl=/dl/whitepapers/Akamai_soti_apac_q310.pdf&solcheck=1&.

[50] "В России DDoS-атака стоит от 200 евро в сутки" [In Russia DDoS Attack Costs 200 Euros Per Day]," iToday.ru, April 5, 2010, http://itoday.ru/news/35916.html (in Russian).

RWANDA

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Partly Free**
Obstacles to Access	n/a	14
Limits on Content	n/a	19
Violations of User Rights	n/a	17
Total	**n/a**	**50**

POPULATION: 10.4 million
INTERNET PENETRATION: 4 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Rwanda's 1994 genocide ravaged the skilled workforce and almost completely destroyed the already poor telecommunications infrastructure, leaving only a handful of telephone lines operational.[1] By 1996, when the state-owned provider Rwandatel first introduced the internet to Rwanda, approximately 1,000 lines were functioning.[2] Mobile phones arrived in 1998, but the usage rate in the first years of access was very low.[3] Since 2000, however, there has been an increase in fixed lines, mobile phones, computers, and technicians in the country. The number of internet users rose from 5,000 in 2000 to 450,000 in 2010, though this is still only 4 percent of the population.[4] More significantly, the number of mobile-phone subscribers grew from only 39,000 in 2000 to over 3 million by 2010, accounting for over a third of the population.[5]

[1] Albert Nsengiyumva and Emmanuel Habumuremyi, *A Review of Telecommunications Policy Development and Challenges in Rwanda* (Johannesburg: Association for Progressive Communications, September 2009), http://www.apc.org/en/pubs/research/review-telecommunications-policy-and-challenges-rw.
[2] Aida Opoku Mensah, "Building an Information Society—The Case of Rwanda," briefing paper, World Summit on the Information Society, United Nations Economic Commission for Africa, November 2005, http://www.uneca.org/aisi/docs/PolicyBriefs/Building%20an%20Information%20Society_the%20case%20of%20Rwanda.pdf
[3] Silas Lwakabamba, "The Development of ICTs in Rwanda: Pioneering Experiences," in *At the Crossroads: ICT Policymaking in East Africa* (Nairobi: East African Educational Publishers/International Development Research Center, 2005), http://www.idrc.ca/en/ev-93064-201-1-DO_TOPIC.html.
[4] Internet World Stats, "Internet Usage Statistics for Africa,", http://www.internetworldstats.com/stats1.htm, accessed February 12, 2011.
[5] "ICT Statistics: September 2010," Rwanda Utilities Regulatory Agency (RURA), http://www.rura.gov.rw/index.php?option=com_content&view=article&id=278, accessed February 12, 2011.

The increased use of the internet and particularly mobile phones has transformed Rwanda, contributing to progress in areas such as education, good governance, human capacity development, and rural community activities. Such progress is expected to continue as part of a government plan to establish Rwanda as a globally competitive knowledge-based society and economy.[6] There have been few attempts to restrict access to content or otherwise limit the use of these technologies. Nevertheless, there are concerns that other restrictions on free expression in the country will seep into the internet sphere, as occurred when the authorities blocked the online version of an independent newspaper in mid-2010. In addition, despite government efforts to enhance access, poverty and lack of appropriate infrastructure, especially in rural areas, continue to impede the expansion of information and communication technologies (ICTs) in Rwanda.

OBSTACLES TO ACCESS

Widespread poverty remains the primary impediment barring Rwandans from accessing new technologies. Over 90 percent of the population lives in rural areas, with the majority practicing subsistence agriculture and approximately 64 percent living below the poverty line. In addition, about 65 percent of the population is illiterate,[7] and between 70 and 90 percent speak only Kinyarwanda.[8] The cost of internet services and private VSAT satellite links has dropped in recent years. Nevertheless, access is still limited mostly to Kigali, the capital city, and remains beyond the economic capacity of most citizens.

In the face of such challenges, the Rwandan government has made ICT development a high priority, spending far more than the average African country on the emerging sector, and instituting incentives like tax exemptions on ICT equipment. Although the full impact has yet to be felt, broadband internet service is progressively replacing dial-up connections, and a study published in July 2010 ranked Rwanda third in Africa for downloading speeds.[9] Broadband connectivity is expected to increase further with the installation of over 100 kilometers of fiber-optic cable and 3.5 gigabytes per second of WiMAX wireless capacity, bringing internet service to the countryside.[10] The recent development of e-government

[6] Glen Farell, "Survey of ICT and Education in Africa: Rwanda Country Report," *info*Dev, April 2007, http://www.infodev.org/en/Document.423.pdf.
[7] UNICEF, "Statistics: Rwanda," http://www.unicef.org/infobycountry/rwanda_statistics.html, accessed August 3, 2010.
[8] Ann Garrison, "Rwanda Shuts Down Independent Press," *Digital Journal*, April 14, 2010, http://www.digitaljournal.com/article/290545; Beth Lewis Samuelson and Sarah Warshauer Freedman, "Language Policy, Multilingual Education, and Power in Rwanda," *Language Policy* 9, no. 3 (June 2010), http://gse.berkeley.edu/faculty/swfreedman/10samuelson_freedman.pdf.
[9] Bridge 2 Rwanda, "Rwanda's Internet Fastest in the Region," July 18, 2010, http://www.bridge2rwanda.org/2010/07/rwanda%E2%80%99s-internet-fastest-in-the-region/.
[10] Emmanuel Habumuremyi and Alan Finlay, "Rwanda's Policy Vacuum Could Mean Trouble for Broadband," Association for Progressive Communications, October 29, 2009, http://www.apc.org/en/news/rwanda-s-policy-vacuum-could-mean-trouble-broadban.

platforms and video conferencing has also shortened travel times, cut expenses, and improved communication among district authorities. Advanced web applications such as the video-sharing site YouTube, the social-networking site Facebook, the microblogging platform Twitter, and international blog-hosting services are freely available.

The mobile-phone penetration rate is significantly higher than that for fixed-line internet access, reaching 36 percent and 3.6 million subscribers as of September 2010,[11] according to official statistics, thereby accounting for the vast majority of telephone users.[12] Access is made easier by a well-developed mobile-phone network covering 92 percent of populated areas.[13] In remote border areas, however, coverage remains faulty or nonexistent. To facilitate greater access, the Rwanda Utilities Regulatory Agency (RURA) is attempting to reduce the price of handsets from 8,000 Rwandan francs (US$14) to 2,000 Rwandan francs (US$3.50).[14] At the current rate of mobile-phone expansion, the number of subscribers is expected to reach six million by 2015, which would be about 60 percent of the population.[15] Internet access via mobile phones has been available since 2007, but the limited bandwidth (approximately 148 kbps) has restrained its popularity. The situation is expected to improve by the end of 2010 due to several ongoing projects, including a fiber-optic cable expansion plan by the public utility company Electrogaz and a project by telecommunications operator New Artel to connect government institutions and low-income segments of the population in rural areas.[16]

Following market liberalization that began in 2001,[17] the number of companies providing telephone and internet services has increased from one—the state-run Rwandatel—to about a dozen in 2010. These include fixed-line providers(Rwandatel, MTN Rwandacell, and Artel International), mobile-phone providers (Rwandatel, MTN Rwandacell, and TIGO), and internet-service providers (ISPA, Rwandatel, MTN Rwandacell, New Artel, Altech Stream Rwanda, Value Data Rwanda, Star Africa Media, Greenmax, Augere Rwanda, and Comium).[18] Rwandatel was partially privatized in 2007, and as of 2010 the government owned only 20 percent of the company. The remainder is owned by LAP Green, a Libyan firm. The other providers are all privately owned.

The Rwanda Information Technology Authority (RITA) and RURA supervise the telecommunications sector. The government appoints the members of both regulatory bodies. In 2009, RURA set up the Rwanda Internet Exchange (RINEX) to connect internet-

[11] "ICT Statistics: September 2010," Rwanda Utilities Regulatory Authority (RURA).
[12] National Institute of Statistics of Rwanda, "Development in ICT Sector."
[13] National Institute of Statistics of Rwanda, "Development in ICT Sector."
[14] "Rwanda Mobile Penetration Hits 24 Percent," Business Monitor International.
[15] Saul Butera, "Mobile Subscribers Reach 2.4 Million," *New Times* (Rwanda), February 12, 2010, http://www.newtimes.co.rw/index.php?issue=14152&article=25176.
[16] Albert Nsengiyumva, Emmanuel Habumuremyi, and Sharon Haba, *Pro-Poor ICT Project Report—Rwanda* (Kigali: Making ICT Work for the Poor, July 2007), http://propoor-ict.net/docs/rwanda_report.pdf.
[17] Nsengiyumva and Habumuremyi, *A Review of Telecommunications Policy Development and Challenges in Rwanda*.
[18] National Institute of Statistics of Rwanda, *ScanICT Baseline Survey Report* (Kigali: National Institute of Statistics of Rwanda, November 2008), http://www.uneca.org/aisi/docs/RWANDA_SCAN_ICT_REPORT.pdf.

service providers (ISPs) and enable local internet communications to be routed through RINEX without having to pass through international networks.[19] ISPs may also opt to connect via RINEX to the international internet. The aim is ostensibly to make intra-Rwandan internet communications cheaper and faster, though such control over internet traffic could also facilitate any future efforts to systematically censor or monitor domestic online communications. As of the end of 2009, only several ISPs were properly connected to RINEX, and the price for national access remained the same as for international.[20]

LIMITS ON CONTENT

Access to online content in Rwanda is generally unfettered. The websites of international human rights organizations such as Freedom House, Amnesty International, and Human Rights Watch, as well as the online versions of media outlets like the British Broadcasting Corporation (BBC), *Le Monde*, Radio France Internationale, and the *New York Times*, are freely accessible. The websites and blogs of opposition activists both within and outside Rwanda are also freely available.[21] Similarly, one of the founders of the online news portal Igihe.com reported no constraints or pressures from the government in establishing and managing that website.[22] Nevertheless, the web versions of state-run media outlets, such as *Imvaho Nshya*, *La Nouvelle Relève*, the Rwanda News Agency, and the *New Times*, dominate the online information landscape.

Despite the generally open online atmosphere, an incident in the months leading up to the August 2010 presidential election raised concerns that the authorities are willing and able to restrict online content. In April, Rwanda's two main independent newspapers, *Umuseso* and *Umuvugizi*, both published in Kinyarwanda, were given six-month suspensions.[23] Although the newspapers were officially suspended for defaming the president and other offenses, the decision was widely perceived as an effort to suppress critical coverage in the run-up to the election. *Umuvugizi*'s editor, who fled into exile, launched an online version in late April, but in early June the Media High Council ordered that the website be blocked, arguing that the ban on the newspaper had to apply online as

[19] Rwanda Utilities Regulatory Agency (RURA), *Guidelines for Rwanda Internet Exchange Point (RINEX) Management* (Kigali: RURA, 2009), http://www.rura.gov.rw/docs/RINEX_GUIDELINES.pdf.
[20] Antoine Bigirimana, "Rwanda: The Story of the Internet—One Step Forward, Two Steps Backward," *New Times*, December 12, 2009, available at http://allafrica.com/stories/200912150559.html.
[21] This includes the website of opposition leader Ingabire Victoire Umuhoza at http://www.victoire2010.com, as well as other sites at http://ww.iwacu1.com, http://ww.musabyimana.be, http://rwandarwabanyarwanda.over-blog.com, and http://ww.banyarwandapoliticalparty.org.
[22] Interview with Founder of Igihe.com in February 2010.
[23] Michael Fairbanks, "Nothing Good Comes Out of Africa," *Huffington Post*, May 3, 2010, http://www.huffingtonpost.com/michael-fairbanks/nothing-good-comes-out-of_b_560639.html; International Freedom of Expression eXchange (IFEX), "Rwanda Shuts Critical Papers in Run-Up to Presidential Vote," news release, April 13, 2010, http://www.ifex.org/rwanda/2010/04/14/papers_suspended/.

well.[24] As of August 2010, the site remained blocked by all ISPs, but by year's end it was available again, as the six-month suspension had expired. The newspaper *Umuseso* does not have an online version. Appealing such a ban is possible based on provisions of the media law, although in this instance, the publications chose not to appeal. Many online journalists based in Rwanda, like their print and broadcast colleagues, engage in self-censorship, particularly on topics that might be construed as disturbing national unity and reconciliation. The High Media Council has been known to contact websites and request that they remove certain information. In addition to *Umuseso* and *Umuvugizi*, this has also reportedly occurred with the online news websites Umusingi and Umurabyo, which have been asked to remove content related to local political affairs and ethnic relations. In terms of the economic environment for online news websites, independent outlets often face challenges gaining advertising from government ministries or state-owned enterprises, as well as benefiting from direct subsidies, which are common sources of income for state-run media. There are no clear regulations outlining treatment of obscene content, but Article 57 of the 2009 Law on Media indicates that cybercafe operators, parents, and business owners are expected to take the lead in preventing minors from viewing websites that display pornography, or information that might incite them to crimes such as drug use or theft. [25]

As internet access has expanded, the Rwandan blogosphere has evolved into a lively space, largely consisting of youth who write on a variety of topics, including their political views. However, opposition supporters living outside Rwanda, especially in Europe and the United States, are responsible for most of the criticism of the government that appears on forums, websites, and blogs. Facebook is also emerging as a popular site for online interaction, with around 70,480 users, of whom 70 percent are between 18 and 34 years of age.[26]

With mobile phones more widely accessible than the internet, text messages have become an important way for citizens to voice discontent with the authorities and expose abuses of power. In one widely reported example in 2009, several local officials and other well-to-do residents stole cows that had been donated by the president for needy residents in the countryside. The theft was reported to local radio stations via text messages, sparking widespread coverage by the media. As a result, the officials were forced to resign or were otherwise punished. Text messages were also used for political mobilization during the 2003 and 2008 elections. In 2010, they enabled the National Electoral Commission to improve voter education and allowed candidates and political parties to mobilize supporters. In particular, contenders from parties other than the ruling party were able to garner more votes than they might have otherwise due to the ability to reach voters via text-messaging

[24] Reporters Without Borders, "Persecution of Independent Newspapers Extended to Online Versions," news release, June 11, 2010, http://en.rsf.org/rwanda-persecution-of-independent-11-06-2010,37718.html.
[25] "Law on Media," *Official Gazette of the Republic of Rwanda*, August 17, 2009, available at http://www.mhc.gov.rw/index.php?option=com_docman&task=cat_view&gid=81&Itemid=144&lang=en.
[26] Facebakers, "Facebook Statistics: Rwanda," www.socialbakers.com/facebook-statistics/rwanda accessed December 29 , 2010.

campaigns.[27] The ability of citizens to use digital media for organizing large-scale "real life" protests remains limited, however, due to broader restrictions on freedom of assembly, particularly regarding politically sensitive topics.

VIOLATIONS OF USER RIGHTS

The Rwandan constitution, adopted in May 2003, provides for freedom of expression. In addition, Chapter IV of the new Law on Media,[28] signed in August 2009, is dedicated to "ICT or internet press" and includes language that explicitly grants freedom for online communications. Article 56 of the law guarantees every person the right to create a website through which he or she can publish "information to a great number of people." Article 58 extends provisions of the law on print and audiovisual materials to ICT communications. While some provisions are irrelevant to online expression, several permissive and restrictive aspects of the legislation may be applicable. These include a prohibition on censorship, on the one hand, and criminal penalties for showing contempt for the president, and restrictions on certain coverage of the executive, judicial, and legislative branches, on the other.

Rwanda's generally restrictive legal environment for traditional media could be applied to the internet, particularly given the lack of a fully independent judiciary. For example, the decision to ban the online version of *Umuvugizi* was based on vague charges of publishing "divisive language,"[29] a category of expression that is criminalized by the 2001 Law on Discrimination and Sectarianism. This provision was also used to ban the print version of *Umuvugizi*, and is often invoked to silence government critics.[30] Similarly, penalties for criminal defamation in print and broadcast media may be applicable to the internet, though they have sparked complaints from media workers and may be revisited and amended in the near future.[31]

Although many traditional journalists view the threat of imprisonment as a key constraint on their work, such punishment is rare for online expression. Idesbald Byabuze, a Congolese journalist and professor who was temporarily teaching in Rwanda, was arrested in February 2007 and held in detention for one month while awaiting trial on charges of

[27] Dominique Nduhura, "Rwanda: Media Coverage of the Parliamentarian Elections (September 15, 2008)," paper presented at the World Journalism Education Congress, Grahamstown/Rhodes University, July 2010, http://wjec.ru.ac.za/index.php?option=com_rubberdoc&view=doc&id=96&format=raw.
[28] "Law on Media," *Official Gazette*.
[29] Media Institute, "Tabloid Website Blocked," IFEX, June 8, 2010, http://ifex.org/rwanda/2010/06/08/umuvugizi_website_blocked/.
[30] Law No. 47/2001 on Prevention, Suppression and Punishment of the Crime of Discrimination and Sectarianism, available at http://www.adh-geneva.ch/RULAC/pdf_state/Law-47-2001-crime-discrimination-sectraianism.pdf; Jennie E. Burnet, "Rwanda," in *Countries at the Crossroads 2007* (New York: Freedom House; Lanham, MD: Rowman and Littlefield, 2007), http://freedomhouse.org/template.cfm?page=140&edition=8&ccrpage=37&ccrcountry=167.
[31] "Law on Media," *Official Gazette*.

"segregation, sectarianism, and threatening national security" for several articles he had written. These included a June 2005 piece about human rights concerns in Rwanda that was published on an overseas website. The charges were dropped after his release, but he was quickly deported from the country.[32] Since 2007, there have been no other reported cases of legal or other harassment for online expression, possibly because most activities by opposition forces are carried out in foreign countries.

In a case that signaled the possibility of violence against print journalists creeping into the online sphere, in June 2010, Jean-Leonard Rugambage, an editor for *Umuvugizi*, the above-mentioned newspaper which was banned in April 2010 but continued to publish online, was assassinated in front of his home in Kigali. Rugambage was the last of the publication's journalists to remain in Rwanda and was reportedly preparing to join colleagues in exile due to threats and intimidation.[33] In November 2010, two individuals were convicted of the killing, claiming it was reprisal for acts of violence Rugambage allegedly committed during the 1994 genocide. However, fellow journalists expressed skepticism over the handling of the case, believing the murder was punishment for critical reporting on the government.[34]

Monitoring of online communications does not appear to be widespread. However, there have been several instances in recent years of e-mails, phone calls, and text messages being produced as evidence in trials; these were mostly obtained via low-tech methods of confiscating suspects' mobile phones and computers rather than via service providers. There have been no reported cases of serious cyberattacks in the country. RURA has initiated a strategy to increase awareness of such threats among business owners and ordinary users.[35]

[32] Bureau of Democracy, Human Rights, and Labor, "Rwanda," in *2007 Country Reports on Human Rights Practices* (Washington, DC: U.S. Department of State, March 2008), http://www.state.gov/g/drl/rls/hrrpt/2007/100499.htm; International Press Institute, "Democratic Republic of Congo," May 8, 2008, http://www.freemedia.at/regions/africa/singleview/4140/.

[33] Danny O'Brien, "Six Stories: Online Journalists Killed in 2010," Committee to Protect Journalists (CPJ), December 17, 2010, http://cpj.org/internet/2010/12/online-journalists-killed-in-2010.php.

[34] "Journalists Killed in 2010: Jean-Léonard Rugambage," Committee to Protect Journalists (CPJ), http://cpj.org/killed/2010/jean-leonard-rugambage.php, accessed February 12, 2011.

[35] Aimable Karangwa, *Cyber Security and CIIP* (Kigali: RURA, n.d.), slides, http://www.rura.gov.rw/publication/Cyber_Security_and_CIIP.pdf, accessed November 22, 2010.

SAUDI ARABIA

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Not Free**
Obstacles to Access	n/a	14
Limits on Content	n/a	27
Violations of User Rights	n/a	29
Total	**n/a**	**70**

POPULATION: 29.2 million
INTERNET PENETRATION: 38 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

The government of Saudi Arabia is credited with supporting the rapid expansion of the internet through consistent upgrades to its infrastructure. However, by implementing strict filtering mechanisms to block undesirable content, excessive monitoring of internet users, and detention and intimidation of online commentators, the government has also been responsible for making the country one of the world's most repressive with respect to freedom of expression online.

Saudis first gained access to the internet on December 15, 1998. Ten years later, the number of internet users in the country had grown to 7.7 million.[1] Today, there are 9.8 million users,[2] making up about 38 percent of the total population. While in the early years the vast majority of Saudi users accessed the internet through dial-up connections,[3] which were often slow and frustrating, only about half of the internet population still uses dial-up service, with the rest using broadband connections.[4]

[1] Communications and Information Technology Commission (CITC), *ICT Indicators in the Kingdom of Saudi Arabia, 2009* (Riyadh: CITC, 2010), http://www.citc.gov.sa/NR/rdonlyres/ECC196FF-D3C1-4C88-B793-685C96CA0309/0/ICTSectorinKSA2009English.pdf.
[2] Ibid.
[3] Internet Services Unit (ISU), "User's Survey," King Abdulaziz City for Science & Technology, 2006, http://www.isu.net.sa/surveys-&-statistics/new-user-survey-results.htm.
[4] CITC, *Internet Usage in the Kingdom of Saudi Arabia: Individuals* (Riyadh: CITC, 2008), http://www.citc.gov.sa/citcportal/GenericListing/tabid/104/cmspid/{FD847314-8EAB-4A52-9B72-9470BC15320D}/Default.aspx.

OBSTACLES TO ACCESS

Internet penetration is highest in major cities like Riyadh and Jeddah, and in oil-rich Eastern Province. Residents of provinces like Jizan in the south and Ha'il in the north are the least likely to use the internet. The younger generations make up the majority of the user population; according to the Communications and Information Technology Commission (CITC), older Saudis often lack the computer literacy to take advantage of the medium.[5] Arabic content is widely available on the internet, as are Arabic versions of applications like chat rooms, discussion forums, and social networking sites. Broadband service costs 270 riyals (US$72) a month on average,[6] representing a sharp drop from the 2003 price of 700 riyals (US$187) a month.[7] Connection speed varies between 128 Kbps for DSL broadband users and 21.6 Mbps for High-Speed Packet Access (HSPA) network users, depending on the service purchased. Connections are considered slow by some, in part because of excessive filtering, but overall infrastructure is not considered a barrier to access except in remote and sparsely populated areas.

According to the CITC, nine out of every ten users access the internet from home, while one-third, mostly working men, access the internet from their place of employment.[8] About 16 percent of the user population frequents internet cafes, which offer a cost-effective alternative. Saudis can also access the internet from their mobile telephones. While five years ago there were fewer than 20 million mobile-phone subscriptions, there are now 44.8 million, for a penetration rate as high as 175 percent.[9]

All forms of internet and mobile-phone access are available in the country, including WiMax broadband, third-generation (3G) mobile networks, internet via satellite, and HSPA technologies. Service for BlackBerry hand-held mobile devices was banned from August 1 to August 10, 2010, due to concerns that the authorities had difficulty accessing its encrypted messages,[10] but the ban was lifted after the company agreed to provide the necessary information.[11] There are roughly 700,000 BlackBerry users in the country.[12] Major video-sharing, social-networking, and microblogging sites like YouTube, Facebook, and Twitter are freely available, as are international blog-hosting services, though specific pages may be blocked.

[5] Ibid., 56.
[6] CITC, *Internet Usage in the Kingdom of Saudi Arabia: Individuals*.
[7] ISU, "User's Survey."
[8] CITC, *Internet Usage in the Kingdom of Saudi Arabia: Individuals*.
[9] CITC, *ICT Indicators in the Kingdom of Saudi Arabia, 2009*.
[10] "Saudi Ban on BlackBerry from Friday," Al-Jazeera, August 4, 2010, http://english.aljazeera.net/news/middleeast/2010/08/2010844243386999.html.
[11] Reuters, "BlackBerry Agrees to Give Saudi Arabia Subscribers' Codes," Al-Arabiya, August 10, 2010, http://www.alarabiya.net/articles/2010/08/10/116289.html (in Arabic).
[12] "Saudi: 48 Hours for BlackBerry Messenger Providers to Try a Suggested Solution," Al-Arabiya, August 7, 2010, http://www.alarabiya.net/articles/2010/08/07/115958.html (in Arabic).

The Internet Services Unit (ISU), a department of King Abdulaziz City for Science & Technology (KACST), is responsible for managing the internet infrastructure in Saudi Arabia. All the retail internet-service providers (ISPs), government organizations, and universities obtain access through the ISU. The entity was established in 1998 and reports to the vice president of KACST. In addition to providing access to the internet, the ISU initially acted as a regulatory body. However, in 2003 the governance of the Saudi internet, including licensing issues, was relegated to the CITC. The CITC is also responsible for regulating the broader information and communication technology (ICT) sector in the country.

The Saudi internet is connected to the international internet through three data-services providers, up from a single gateway in years past. These providers offer service to licensed ISPs, which in turn sell connections to dial-up and leased-line clients. The number of ISPs in the country has risen from 23 in 2005 to 53 in 2009. Broadband and mobile-phone services are provided by the three largest telecommunications companies in the Middle East—Saudi Telecom Company (Saudi Arabia), Etisalat (United Arab Emirates), and Zain (Kuwait). WiMax broadband, a technology that allows users to access the internet from any location using USB modems, is widely used in Saudi Arabia.

LIMITS ON CONTENT

The Saudi government subjects internet content to strict filtering. Sites that contain harmful, illegal, anti-Islamic, or offensive material are blocked, as are those that carry criticism of Saudi Arabia, the royal family, or the other Gulf states. Material providing information about drugs, alcohol, gambling, or terrorism, and sites that call for political reform or are critical of the current social landscape, are also blocked. While the rules governing internet usage are clearly stated on government websites, allowing internet users to discern what is expected of them, the Saudi authorities often disregard their own guidelines by blocking sites that are not explicitly covered. The OpenNet Initiative's 2009 testing results showed that Saudi Arabia also blocks human rights websites like Article19.org, Saudihr.org, andHummum.net.[13] Although the country's internet access now flows through three nodes—operated by the Saudi Telecom Company, Integrated Telecom Company, and Bayanat al-Oula for Network Services—instead of a single node as in the past, the three data-service providers must all block the sites banned by the CITC.[14]

Filtering in Saudi Arabia takes place at the country-level servers of the three data-service providers. These servers, which contain long lists of blocked sites, are placed

[13] OpenNet Initiative, "Country Profile: Saudi Arabia," August 6, 2009, http://opennet.net/research/profiles/saudi-arabia.
[14] CITC, "Content Filtering in Saudi Arabia," http://www.internet.gov.sa/learn-the-web/guides/content-filtering-in-saudi-arabia, accessed September 30, 2010.

between the state-owned internet backbone and servers in the rest of the world. All user requests that arrive via Saudi ISPs travel through these servers, where they can be filtered and possibly blocked. Users who attempt to access a banned site are redirected to a page that informs them of the site's status, meaning the government is at least partly transparent about the content it blocks. However, the list of banned sites is not publicly available, and the government also responds to takedown notices from members of the public, who can alert the government to undesirable material.[15] Members of the public have the opportunity to unblock sites through a similar system designated for this purpose.[16] Once an individual submits a request to unblock a site by completing a web-based form, a team of CITC employees determines whether the request is justified. The CITC is believed to receive hundreds of such requests each day.

The CITC claims that the time lost determining whether a user's site request should be blocked or allowed is not more than half a second. However, a survey conducted by the commission in 2008 showed that 33 percent of internet users in the country, particularly younger participants and women, found content filtering problematic.[17] These users complained that filtering denied them access to a great deal of useful information and limited their ability to browse freely.

The Saudi blogosphere is not as active as other online platforms for political discussion in the country. For example, while there are an estimated 10,000 Saudi bloggers, many more Saudis use Facebook. There are more female than male bloggers in Saudi Arabia, and most bloggers tend to focus on personal matters rather than local politics. However, online public discussion forums have always been popular, and their effect has been quite significant. These online communities have continued to receive unmatched attention even after the emergence of social-networking and blog-hosting applications. The forums give ordinary individuals from all backgrounds the opportunity to express themselves and get their messages across even to the country's leadership. It is believed that the king fired several ministers for negligence, corruption, or incompetence in 2009 based on evidence posted on Al-Saha al-Siyasia,[18] the most popular online political forum in Saudi Arabia. Countless other incidents have demonstrated the ability of online commentators to steer the government's attention to particular problems.

Sites like YouTube and Facebook provide additional media platforms with minimal government control. Saudis used YouTube very effectively during major floods in Jeddah in 2009, which resulted in 120 deaths. They not only posted hundreds if not thousands of videos capturing the tragedy as it occurred, but also demanded action from the authorities.

[15] The CITC block-request form is available at http://www.internet.gov.sa/resources/block-unblock-request/block/view?set_language=en.
[16] The CITC unblock request form is available at http://www.internet.gov.sa/resources/block-unblock-request/unblock/.
[17] CITC, *Internet Usage in the Kingdom of Saudi Arabia: Individuals*.
[18] Agence France-Presse, "Saudi Reshuffle Puts Woman in Ministry," *Australian*, February 16, 2009, http://www.theaustralian.com.au/news/saudi-reshuffle-puts-woman-in-ministry/story-e6frg6tx-1111118859647; Al-Saha al-Siyasia is located at http://www.alsaha.com/sahat/4.

In response, the king immediately established a commission to investigate the disaster, which was apparently an unprecedented move. While YouTube was credited with exposing the scandal of the floods,[19] many Saudis then used Facebook to organize themselves and assist with rescue efforts, taking an important step toward greater civic and political activism in the country.[20]

Al-Saha al-Siyasia is not accessible from inside Saudi Arabia because of the sensitive nature of the topics discussed on it, and particular pages on YouTube and Facebook are also blocked. The sites nevertheless mean a great deal to many Saudis due to the dearth of other channels for free expression.

VIOLATIONS OF USER RIGHTS

Saudi Arabia's basic law contains language that provides for freedom of speech and freedom of the press, but only within certain boundaries. The 2000 Law of Print and Press addresses freedom of expression issues, but it largely consists of restrictions rather than protections. The government treats online journalists writing for newspapers and other formal news outlets the same as print and broadcast journalists, subjecting them to close supervision. Bloggers and online commentators who write under pseudonyms face special scrutiny from the authorities, who attempt to identify and punish them for critical or controversial remarks. Online writers are often arrested and detained without specific charges, though it is frequently clear which views offended the government. The Ministry of Interior, headed by Prince Naif bin Abdulaziz al-Saud, has generally enjoyed impunity for abuses against bloggers and online commentators.

In response to a series of hacking attacks, including one on the Ministry of Labor in 2008,[21] the government has enacted laws that criminalize a range of internet-based offenses. The vaguely worded legislation assigns jail sentences and fines for defamation; unauthorized interception of private e-mail messages; hacking a website to deface, destroy, modify, or deny access to it; or simply publishing or accessing data that is "contrary to the state or its system." Many online commentators have been imprisoned under these laws after harshly criticizing the government or expressing support for terrorism.

Critical journalism is not tolerated in the country. In July 2008, when the editor in chief of a local newspaper asked Prince Naif a question that contained implicit criticism of

[19] Amira al-Hussaini, "Saudi Arabia: The Jeddah Floodings on Video," Global Voices, December 17, 2009, http://globalvoicesonline.org/2009/12/17/saudi-arabia-the-jeddah-floodings-on-video/.
[20] Paul Handley, "Outraged Saudis Blast Govt after Deadly Jeddah Flood," Agence France-Presse, November 28, 2009, available at http://www.google.com/hostednews/afp/article/ALeqM5ji17eEs80JpewJ4n0Py-7gQY5UTA.
[21] "Unemployed Man Hacks into Ministry of Labor and Parliament and Asks Private Sector to Employ Him," *Al-Madina*, September 3, 2008 (in Arabic).

the religious police, the prince scolded him and he resigned the following day.[22] Anonymous online commentators commonly make defamatory remarks; while only a few choose to press charges against writers who publicly vilify them, it is understood that the government could arrest those writing from inside the country. In September 2010, the government announced its intent to require all online publishers and media, including bloggers and online forums, to obtain a license from the government.[23] The spokesperson of the Minister of Information and Culture claimed that the measure was necessary to curb defamation and libel.

Surveillance is rampant in Saudi Arabia. Everyone using communication technology is subject to government monitoring, which is aimed at protecting national security and maintaining social order. The authorities regularly monitor websites, blogs, chat rooms, as well as the content of e-mail and mobile-phone text messages. Users are not able to purchase mobile phones anonymously. They are legally required to use their real names or register with the government, and the authorities can obtain identification data without a court order or similar legal process.

The short-lived ban on BlackBerry service in August 2010, which ended when the government obtained the means to access the devices' encrypted messages, clearly suggested that all other electronic media were already under the watchful eye of the authorities.[24] Moreover, the blocking of the Twitter pages of two human rights activists, Khaled al-Nasser and Walid Abdelkhair, on August 20, 2009, demonstrated the government's diligence in restricting content, as Twitter is not particularly popular in Saudi Arabia.

Dozens if not hundreds of alleged extremists have been arrested after apparently drawing the authorities' attention through activity on online forums. The Ministry of Interior is believed to be the main government body responsible for monitoring extremist content. The resulting arrests without formal charges mean that detainees cannot defend themselves or secure legal representation. Some online commentators have reported that the authorities confiscated their computers and never returned them.

In addition to direct government monitoring, access providers are also required to monitor their customers and supply the authorities with information about their online activities. On April 16, 2009, the Ministry of Interior made it mandatory for internet cafes to install hidden cameras and provide identity records for their customers. The new security regulations also barred anyone under 18 years of age from using internet cafes. All internet cafes were ordered to close by midnight, and police were instructed to visit the businesses to ensure compliance. These measures were ostensibly designed to crack down on internet

[22] "Prince Naif Responds to the 'Spiteful' Journalist Ahmed al-Yousef," YouTube, July 4, 2008, video, http://www.youtube.com/watch?v=RB4JnaK-LZY&feature=related.
[23] Alexia Tsotsis,"Saudi Arabians Will Soon Need a License to Blog," TechChrunch, September 23, 2010, http://techcrunch.com/2010/09/23/saudi-arabians-will-soon-need-a-license-to-blog/#.
[24] Reuters, "BlackBerry Agrees to Give Saudi Arabia Subscribers' Codes."

use by extremists, but in practice they allow the police to deter any activity that the government may find objectionable.

Several media websites and portals have been subject to cyber attacks in recent years. The website of the satellite television station Al-Arabiya was attacked in 2009 by a hacker seeking retribution for content deemed offensive to Shiites. The website of the newspaper *Al-Watan* was hacked twice in 2009 because of its criticism of religious scholars. Even high-profile online commentators' pages and forum accounts have been hacked. The Facebook pages of the prolific Saudi judge Eisa al-Ghaith have been disrupted several times. The forum account of well-known progovernment commentator Al-Bahbahari has also been hacked by critics of his loyalist stance.

Online commentators who express support for extremism or liberal ideals, call for strikes, argue in favor of the rights of Shiites and other minorities, call for political reform, or expose human rights violations are perceived as threats by the regime. Although data on the exact number of those arrested are not publicly available, several prominent bloggers and activists are known to have been detained in recent years. In 2007, the Ministry of Interior arrested the popular blogger Fuad al-Farhan because of his consistent advocacy for political reforms. He was released in April 2008. Between 2008 and 2009, the Ministry of Interior arrested bloggers including Youssef Ashmawy, Raafat al-Ghanim, Roshdi Algadir, Mohammed Otaibi, and Khaled al-Omair; most of these individuals have since been released. Munir al-Jassas, a Saudi activist and defender of the rights of Shiites, remains behind bars after being arrested on November 7, 2009. Another defender of the Shiite minority, Mekhlef bin Dahham al-Shammari, has been in custody since June 15, 2010, when he was arrested for criticizing political and religious leaders.

SOUTH AFRICA

	2009	2011
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access	7	7
Limits on Content	8	9
Violations of User Rights	9	10
Total	**24**	**26**

POPULATION: 49.9 million
INTERNET PENETRATION: 9 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Digital media freedom is generally respected in South Africa. Political content is not censored, and bloggers are not prosecuted for online activities. Access to the internet has improved; in fact, more people have an option to access the internet from their mobile telephones than from computers. Nevertheless, the majority of the population is unable to benefit from internet access due to high costs and the fact that most content is in English, an obstacle for those who speak only local languages. There are increasing concerns about laws and legal cases, as well as disciplinary cases in the workplace that may negatively affect digital media freedom, although the courts have been reluctant to infringe on this freedom.

The first internet connection in South Africa was established in 1988, when an email link was set up by academics using the FidoNet mailing system, followed by a Unix-to-Unix Copy (UUCP) gateway. The early days of networking were driven by the Foundation for Research Development and a loose grouping of individuals in various universities.[1] The internet diffused rapidly among the country's technologically advanced elite, especially once it was commercialized from 1993 onwards. By the mid 1990's, South Africa ranked higher in internet usage than other countries at comparable levels of development. Today, South Africa maintains the greatest level of internet penetration in the region, although from a global perspective, the overall level of access is quite modest.

[1] Lawrie, M. 'The history of the internet in South Africa: how it began', http://www.aug.co.za/PPTFiles/The%20History%20of%20the%20Internet%20in%20South%20Africa.pdf, accessed 17/08/2010.

OBSTACLES TO ACCESS

Access to the internet has steadily improved in South Africa despite the obstacles that remain, and options for access are proliferating rapidly. It is estimated that about five million people, or 10 percent of the population, have access, and the penetration rate accelerated in 2008 and 2009. This growth has been attributed to the completion in mid-2009 of the new Seacom undersea cable, the granting of Electronic Communications Network Service licenses to more than 400 organizations since a landmark August 2008 court ruling that value-added network service (VANS) providers can self-provide facilities, and the continued uptake of broadband services by small and medium-sized businesses.[2]

Prices remain a significant barrier to internet access, especially for users of prepaid services. The cost of dial up subscription varies from 40 to 180 South African rands (approx. US$5 to US$24), whereas ADSL subscription is between 50 and 200 rands (approx. US$7 to US$27). Those with access, especially broadband access, are concentrated in urban areas. However, after years of stifled competition, the market is slowly opening up, and it is expected that costs will drop even further thanks to the arrival of the Seacom cable and the completion of the East African Submarine System (Eassy) cable, as well as the increasing use of updated mobile-telephone technology and the laying of new fiber-optic cable within and between cities.[3] In fact, although the overall figures remain very low,[4] the number of South Africans accessing the internet through a broadband connection has grown by more than 50 percent since March 2009,[5] and wireless broadband access has grown by 88 percent in the same period.[6] Telkom SA, a partly stated-owned company, retains a near monopoly in providing broadband access via ADSL, though the recent licensing of a second national operator, Neotel, should increase competition. In March 2010, the internet-service provider (ISP) M-Web launched an uncapped ADSL offering, unleashing a price war in the ADSL market.[7]

[2] World Wide Worx, "SA Internet Growth Accelerates," news release, January 14, 2010, http://www.worldwideworx.com/archives/234, accessed June 4, 2010.
[3] Candice Jones, "More Bandwidth Coming," ITWeb, March 30, 2010, http://www.itweb.co.za/index.php?option=com_content&view=article&id=31713:more-bandwidth-incoming&catid=147&Itemid=68, accessed June 4, 2010.
[4] South Africa currently has a broadband penetration of 4 connections per 100 inhabitants. For more information, see "SA's broadband penetration: the way forward", MyBroadband, October 13, 2010, http://mybroadband.co.za/news/broadband/15804-SAs-broadband-penetration-The-way-forward.html.
[5] World Wide Worx, "Broadband Speeding Ahead," news release, March 17, 2010, http://www.worldwideworx.com/archives/243, accessed June 4, 2010.
[6] Ibid.
[7] Candice Jones, "Another Salvo in Broadband War," ITWeb, May 5, 2010, http://www.itweb.co.za/index.php?option=com_content&view=article&id=32837:another-salvo-in-broadband-war&catid=147&Itemid=68, accessed June 6, 2010.

There are five mobile-phone companies in South Africa—Vodacom, MTN, Cell-C, Virgin Mobile and 8ta—all of which are privately owned, save for 8ta, which is owned by Telkom. The state previously owned a stake in Vodacom through Telkom, but the shares have been disposed of. Privately owned ISPs number in the hundreds. The State Information Technology Agency provides internet services to the government.

Broadband access is also available via mobile phones. South Africa is in an unusual position in that some mobile broadband packages are cheaper than the fixed-line alternative. However, less than half of urban mobile users who have internet-capable phones actually use the internet; most who do use internet capabilities focus on specific applications like the Mxit instant-messaging service and the social networking facility Facebook Mobile rather than regular browsing.[8] The total number of mobile-phone subscribers is estimated to be 32.498 million, or 71.3 percent of the adult population.[9]

The government has not imposed restrictions on internet access, and there have been no reports that the authorities use control over internet infrastructure to limit connectivity. Individuals and groups can engage in peaceful expression of views via the internet using e-mail, instant messaging, chat rooms, and blogs. The video-sharing site YouTube, Facebook, and international blog-hosting services are freely available.

The autonomy of the Independent Communications Authority of South Africa (ICASA) is protected by the South African constitution, although several incidents involving ministerial policy directives sent to the regulator have called the extent of its independence into question.[10] It has been accused of favoring the dominant companies, including Telkom. Access providers and other internet-related groups are self-organized and quite active in lobbying the government for better legislation and regulations, including measures that would upgrade the independence and capacity of ICASA.

LIMITS ON CONTENT

While internet content remains largely free of government censorship, a recent amendment to the Films and Publications Act of 1996 has raised fears that controversial content could be restricted. The amendment, which was passed into law in 2009, requires that every print and online publication that is not a recognized newspaper be submitted for classification to the government-controlled Film and Publications Board if it includes depictions of "sexual conduct which violates or shows disrespect for the right to dignity of any person, degrades a

[8] World Wide Worx, "Mobile Internet Booms in SA," news release, May 27, 2010, http://www.worldwideworx.com/archives/250, accessed June 4, 2010.
[9] South African Advertising Research Foundation, "AMPS Trended Media Data: Cellphone Trends," http://www.saarf.co.za/, accessed June 4, 2010.
[10] Open Society Initiative for Southern Africa, *South Africa*, Public Broadcasting in Africa Series (Johannesburg: Open Society Initiative for Southern Africa, 2010).

person, or constitutes incitement to cause harm; advocates propaganda for war; incites violence; or advocates hatred based on any identifiable group characteristic and that constitutes incitement to cause harm." Exemptions are provided for artistic and scientific speech, but the board has the discretion to grant or deny these exemptions.[11]

In May 2010, the deputy minister of home affairs, Malusi Gigaba, announced that he had approached the country's Law Reform Commission to ask for a complete ban on digitally distributed pornography at the first tier of service providers, through an internet and mobile-phone pornography bill developed by the Justice Alliance of South Africa. The bill uses a very broad definition of pornography found in a law outlawing sexual offenses.[12] Gigaba was quoted by the British Broadcasting Corporation (BBC) as saying: "Cars are already provided with brakes and seatbelts…. There is no reason why the internet should be provided without the necessary restrictive mechanisms built into it."[13]

Apart from the areas mentioned above, the government does not restrict material on contentious topics such as corruption and human rights. Citizens are able to access a wide range of viewpoints, and there are no government efforts to limit discussion. Online content, however, does not match the diverse interests within society, especially with respect to race and local languages. There are a number of political and consumer-activist websites, though the internet is not yet a key space for social or political mobilization.

The South African blogosphere has been highly active in promotion of AIDS awareness and the discussion of environmental issues, in addition to more general political coverage. Mobile phones are used for political organization, especially during recent developments like the establishment of the new political party Congress of the People (COPE), a breakaway faction of the ruling African National Congress (ANC). The main political parties that ran in the 2009 national elections also developed online campaigns to attract young voters, drawing inspiration from U.S. president Barack Obama's use of internet platforms in his 2008 campaign.[14]

Radio, followed by television, continue to be the main sources of news and information for most South Africans, but there are increasing efforts to extend mainstream news outlets to online platforms. The *Times* and *Mail & Guardian* newspapers, for example, operate affiliated websites. All major media groups now have an online presence.

[11] Films and Publications Amendment Act, No. 3 of 2009, http://www.info.gov.za/view/DownloadFileAction?id=106329, accessed June 4, 2010.
[12] Criminal Law (Sexual Offences and Related Matters) Amendment Act, No. 32 of 2007, http://www.info.gov.za/view/DownloadFileAction?id=77866, accessed June 4, 2010.
[13] "Porn Ban on Net and Mobiles Mulled by South Africa," BBC, May 28, 2010, http://news.bbc.co.uk/2/hi/technology/10180937.stm.
[14] J. Duncan, "Desperately Seeking Depth: The Media and the 2009 Elections," in *Zunami! The 2009 South African Elections*, ed. R. Southall and J. Daniel (Johannesburg: Jacana Media, 2009).

VIOLATIONS OF USER RIGHTS

The constitution guarantees "freedom of the press and other media; freedom to receive or impart information or ideas; freedom of artistic creativity; and academic freedom and freedom of scientific research." However, it also includes constraints, and freedom does not extend to "propaganda for war; incitement of imminent violence; or advocacy of hatred that is based on race, ethnicity, gender, or religion and that constitutes incitement to cause harm."[15] The judiciary in South Africa is independent and has issued at least one ruling protecting freedom of expression online.

Libel is not a criminal offense, but civil laws have been applied to online content. Moreover, criminal law has been invoked on at least one occasion to prosecute for injurious material. In January 2009, an Eldorado Park resident, Duane Brady, was fired by his employer and arrested for *crimen injuria*, a common-law offense entailing the deliberate injury of a person's reputation or invasion of privacy, after he insulted his wife's friend on Facebook. The case intensified an ongoing debate about freedom of expression and its limitation on social networking sites, especially when it came to employees defaming their employers online. The issue had first come to the fore in 2007, when a blogger, Llewellyn Kriel, was fired by the media firm Avusa for criticizing his immediate employer, the *Sowetan* newspaper.[16]

Threats to media freedom have also extended to the online content of newspapers. For instance, in May 2009, the country's public broadcaster, the South African Broadcasting Corporation (SABC), filed a charge of "stolen property" after the *Mail & Guardian* posted on its website a documentary on political satire that the broadcaster had refused to air. The documentary explored the fact that award-winning cartoonist Zapiro is being sued by President Jacob Zuma for portraying him about to rape Lady Justice. The newspaper's editor, Nic Dawes, argued that he and his colleagues had a professional duty to make such material public, and accused the SABC of censorship.[17]

In May 2010, the South African Council of Muslim Theologians attempted to stop the *Mail & Guardian* from publishing a cartoon by Zapiro that depicted the prophet

[15] Constitution of the Republic of South Africa, May 8, 1996, Bill of Rights, Chapter 2, Section 16.
[16] "Legal Cases from Facebook Usage Rise," IT News Africa, November 30, 2009, http://www.itnewsafrica.com/?p=3380, accessed June 4, 2010; Arthur Goldstuck, "Fired for Blogging," *Amablogoblogo*, November 30, 2007, http://www.thoughtleader.co.za/amablogoblogo/2007/11/30/fired-for-blogging/.
[17] Matthew Burbidge, "SABC Lays Charge of 'Theft' over Zapiro Doccie," *Mail & Guardian*, May 28, 2009, http://www.mg.co.za/article/2009-05-28-sabc-lays-charges-of-theft-over-zapiro-doccie, accessed June 6, 2010.

Muhammad, arguing that the image was insulting to Muslims. A court injunction, which would have extended to the online version of the newspaper, was not granted.[18]

There have been no reports that the government monitors e-mail or internet chat rooms, except to combat child pornography. Recent legislation potentially allows for extensive monitoring, and was in force as of June 2009. The Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 (RICA) requires ISPs to retain customer data for an undetermined period of time and bans any internet system that cannot be monitored. In addition, the Electronic Communications and Transactions Act of 2002 (ECTA) created a legion of inspectors trained to "inspect and confiscate computers, determine whether individuals have met the relevant registration provisions as well as search the Internet for evidence of 'criminal actions."[19]

Mobile subscribers are required to provide extensive personal information to service providers, and the data are then made available to the government. An identification number is legally required for any SIM-card purchase, although this law appears to be enforced unevenly, and people already in the possession of SIM cards are required to register these cards and provide proof of residence and an identity document by the end of 2010.[20]

The ECTA also requires ISPs to respond to and implement take-down notices (TDNs) regarding illegal content, such as child pornography, material that could be defamatory without justification, or copyright violations. The law states that ISPs "do not have an obligation to monitor," exempting them from liability if proscribed content is found on their service but taken down once a notice is received. However, this exemption only applies if the ISPs are members of a recognized representative organization. The Ministry of Communications has recognized the Internet Service Providers' Association of South Africa (ISPA) as an industry representative body under the ECTA. The ISPA acts as an agent on behalf of its 160 members and provides the ministry with annual information about the total number of TDNs issued, the actions taken in response, and the final results.[21] Most of the complaints lodged are resolved amicably, with ISPA's clients agreeing to take down the offending content.[22]

---

[18] "Anger Mounts Over Zapiro Cartoon," *Mail & Guardian*, May 22, 2010, http://www.mg.co.za/article/2010-05-22-anger-mounts-over-zapiro-cartoon, accessed June 24, 2010.

[19] Privacy International, "South Africa," in *Silenced: An International Report on Censorship and Control of the Internet* (London: Privacy International, 2003), http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-103781, accessed June 24, 2010.

[20] Nicola Mawson, "'Major' RICA Threat Identified," ITWeb, May 27, 2010, http://www.itweb.co.za/index.php?option=com_content&view=article&id=33518:major-rica-threat-identified&catid=69&Itemid=58, accessed June 8, 2010.

[21] Paul Vecchiatto, "Content Disputes Settled Amicably," ITWeb, March 12, 2010, http://www.itweb.co.za/index.php?option=com_content&view=article&id=31260%3Acontent-disputes-settled-amicably&catid=182%3Alegal-view&Itemid=58, accessed June 8, 2010.

[22] "Nyanda Recognises ISPA as Industry Representative Body," BizCommunity.com, May 21, 2009, http://www.bizcommunity.com/Article/220/16/36156.html, accessed June 8, 2010.

RICA provides for an "interception direction" that obliges ISPs to send the communications in question to an interception center. However, the law requires judicial oversight and includes guidelines for judges to establish whether the interception is justified in terms of proportionality and narrowly defined standards.

Reports indicate that the government conducts some surveillance of mobile-phone conversations and short-message service (SMS) or text messages. The National Communications Centre (NCC) reportedly has the technical capabilities and staffing to monitor both SMS and voice traffic originating outside South Africa.[23] Calls from foreign countries to recipients in South Africa can allegedly be monitored for certain keywords; the NCC then intercepts and records flagged conversations. While most interceptions involve reasonable national security concerns, such as terrorism or assassination plots, the system allows the NCC to record South African citizens' conversations without a warrant.[24]

There have been no reports of extralegal intimidation targeting online journalists, bloggers, or other digital-technology users by state authorities or any other actor.

[23] Moshoeshoe Monare, "Every Call You Take, They'll Be Watching You," *Independent*, August 24, 2008, http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=vn20080824105146872C312228, accessed March 27, 2009.
[24] Ibid.

SOUTH KOREA

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Partly Free**
Obstacles to Access	n/a	3
Limits on Content	n/a	12
Violations of User Rights	n/a	17
Total	**n/a**	**32**

POPULATION: 48.9 million
INTERNET PENETRATION: 82 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Free

INTRODUCTION

South Korea's internet infrastructure is one of the most advanced in the world, and its democratic institutions—including an independent judiciary—generally protect free expression. However, regulatory measures such as a real-name registration system and a recent series of arrests of bloggers have presented challenges to internet freedom. The United Nations special rapporteur on freedom of expression and international human rights groups have voiced concerns that the space for free expression has been diminishing since protests against American beef imports that broke out in 2008.[1]

South Korea's high internet penetration rate is widely attributed to a series of state-led initiatives implemented since the 1990s, such as Cyber Korea 21 (1999–2002), the e-Korea Vision 2006 (2002–2006), and the U-Korea Master Plan (2006–2010). The government's rationale for this policy of nationwide promotion of information and communication technologies (ICTs) is that a country with few natural resources like South Korea must move quickly toward a knowledge-based economy if it is to compete with

[1] Frank La Rue, "Full Text of Press Statement Delivered by UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Mr. Frank La Rue, After the Conclusion of His Visit to the Republic of Korea," United Nations Office of the High Commissioner for Human Rights, May 17, 2010, http://www2.ohchr.org/english/issues/opinion/docs/ROK-Pressstatement17052010.pdf; Irene Khan, "Statement by Irene Khan, Amnesty International Secretary General, on the Completion of Her Visit to South Korea," Amnesty International, November 24, 2009, http://www.amnesty.org/en/library/asset/ASA25/013/2009/en/81c8df37-c1d9-4d49-aa8c-825cd7ce9203/asa250132009en.pdf; Reporters Without Borders, *Enemies of the Internet—Countries Under Surveillance* (Paris: Reporters Without Borders, March 12, 2010), http://en.rsf.org/IMG/pdf/Internet_enemies.pdf.

established economic powers.[2] Cyber Korea 21 was well received by the Korean public, partly because such a rationale appealed to them in the aftermath of the Asian financial crisis of 1997, and partly because a foundation of computer-mediated communications had already been laid. In the late 1980s and early 1990s, the *PC tongshin* (PC communication) culture had thrived, using an early, text-based form of online communication comparable to the Minitel in France. The half-dozen *PC tongshin* service providers then helped ease the Korean public onto the internet, the commercialization of which began around 1994.

OBSTACLES TO ACCESS

South Korea is one of the most wired countries in the world, in terms of both internet penetration and high connection speeds. As of 2009, there were an estimated 39.4 million users, comprising about 80 percent of the population.[3] According to the National Bureau of Statistics, as of December 2010, over 80 percent of households had access to the internet,[4] and nearly all connections are broadband. The country has not only the highest number of broadband connections per capita in the world but also the world's highest rate of WiFi hotspots per capita, with 55,000 hotspots in place throughout the country by the end of 2010.[5] Several factors have contributed to the country's high level of connectivity. First, high-speed connections are relatively affordable. Most residences have connections capable of reaching 100 mbps for a cost of around 30,000 won (US$28) per month.[6] Second, the population is highly concentrated in urban areas. Roughly 70 percent of South Koreans live in cities dominated by high-rise apartment buildings that can easily be connected to fiber-optic cables.[7] Finally, the government has carried out programs to expand infrastructure and access, including subsidies to provide access to low-income groups.[8] In terms of mobile-

[2] National Computerization Agency, *Informatization White Paper 2002: Global Leader e-Korea* (Seoul: NCA, 2002), http://www.itglobal.or.kr/_file/m_board/download.asp?file=%BF%B5%B9%AE_b2002eng.pdf.

[3] International Telecommunication Union, "ICT Statistics 2009: Estimated Internet Users, Fixed Internet Subscriptions, Fixed Broadband Subscriptions," ITU ICT Eyes, 2009, http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

[4] "Households with Access to the Internet and Access to a Home Computer," e-National Indicators, December 6, 2010, http://www.index.go.kr/egams/stts/jsp/potal/stts/PO_STTS_IdxMain.jsp?idx_cd=1345&bbs=INDX_001 (in Korean). According to the latest OECD Key ICT Indicators, the figure nears 96 percent of the households when internet access through devices other than computers is also included. "Households with Access to the Internet in Selected OECD Countries," OECD Key ICT Indicators, December 24, 2010, http://www.oecd.org/dataoecd/19/45/34083073.xls.

[5] "Number of WiFi Hotspots in S. Korea Rises to World's No. 3," *Yonhap News*, November 7, 2010, http://english.yonhapnews.co.kr/techscience/2010/11/05/49/0601000000AEN20101105007300320F.HTML.

[6] John D. Sutter, "Why Internet Connections Are Fastest in South Korea," *CNN Tech*, March 31, 2010, http://articles.cnn.com/2010-03-31/tech/broadband.south.korea_1_broadband-plan-south-korea-broadband-internet?_s=PM:TECH.

[7] J. C. Herz, "The Bandwidth Capital of the World," *Wired* (August 2002), http://www.wired.com/wired/archive/10.08/korea.html?pg=1&topic=&topic_set.

[8] Sutter, "Why Internet Connections Are Fastest in South Korea."

phone penetration, as of December 2010, there were 50.8 million subscriptions, exceeding the total population of 48.9 million.[9] More than 56 percent of these users have been accessing the internet from their mobile phones.[10] Smartphone ownership has grown exponentially, reaching the world's highest average traffic per user on smartphones at 271 MB/month, 2 to 3 times higher than the global average.[11]

There is no significant gap in access to ICTs with respect to gender or income level,[12] although differences in computer literacy across generational and professional lines persist.[13] In addition to the high household subscription rates, the absence of a large digital divide is attributable to the omnipresence of cybercafes, known as *PC bangs* (PC rooms) in Korean. The facilities offer broadband access at a price of approximately US$1 per hour, and also serve as venues for social interaction, particularly among youth, who frequent the cafes to play online video games.[14]

Despite such widespread connectivity, some obstacles to access remain. For example, foreign residents have difficulty accessing many online services, both governmental and commercial.[15] This is partly due to language barriers, but a more important factor is the real-name registration system adopted in 2004 under an amendment to the Public Official Election Act.[16] Users are required to verify their identities by submitting their Resident Registration Numbers (RRNs) when they wish to join and contribute to web portals and other major sites. As RRNs are assigned only to Korean citizens at birth, foreign nationals must individually contact webmasters to confirm their identities.

In 2007, the internet real-name registration system was expanded to apply to any website with more than 100,000 visitors per day.[17] This included the video-sharing website YouTube, but the site's U.S.-based parent company, Google, refused to ask its Korean customers for their RRNs. Instead, it has blocked users from uploading content onto YouTube Korea. Users are able to bypass the restriction by changing their location setting to

[9] Korea Communications Commission, "Wired/Wireless Subscriptions December 2010," Resources: Statistical Data, January 25, 2011, http://www.kcc.go.kr/user.do?mode=view&page=P02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=30693 (in Korean).

[10] Korea Internet and Security Agency, *2010 Survey on Wireless Internet Usage* (Seoul: KISA, December 2010), http://isis.kisa.or.kr/board/index.jsp?pageId=040100&bbsId=7&itemId=773&pageIndex=1 (in Korean).

[11] "Smartphones Account for Almost 65% of Mobile Traffic Worldwide," Informa Telecoms & Media, November 2, 2010, http://www.informatm.com/itmgcontent/icoms/s/press-releases/20017822478.html.

[12] Korea Internet and Security Agency, *2010 Survey on Internet Usage* (Seoul: KISA, December 2010), http://isis.kisa.or.kr/board/index.jsp?pageId=040100&bbsId=7&itemId=771&pageIndex=1 (in Korean).

[13] G. W. Shin, J. H. Goh, et al., *2009 Digital Divide Index* (Seoul: National Information Society Agency, 2010), http://www.nia.or.kr/Extra/Module/Common/Lib/Attach/DownLoad.aspx?Seq=18459 (in Korean).

[14] Herz, "The Bandwidth Capital of the World"; Jun-Sok Huhh, "Culture and Business of PC Bangs in Korea," *Games and Culture* 3, no. 1 (2008): 26–37.

[15] Korea Internet and Security Agency, *2010 Survey on the Internet Usage of Foreign Residents in Korea* (Seoul: KISA, December 2010), http://isis.kisa.or.kr/board/index.jsp?pageId=040100&bbsId=7&itemId=770&pageIndex=1 (in Korean).

[16] The amendment became Article 82, Provision 6 of the act.

[17] The expansion was a result of the Act on Promotion of Information and Communications Network Utilization and Data Protection.

"worldwide." Even the Korean presidential office maintains its YouTube channel in this way.[18] Other popular applications such as the social networking site Facebook and the microblogging service Twitter are freely available, and these international sites are currently exempt from the identity verification requirement. Although subject to the real-name registration system, locally based social networking sites like Cyworld and web portals like Naver and Daum are also popular among Korean users.

The telecommunications sector in South Korea is relatively diverse and open to competition, with 127 internet service providers (ISPs) operating as of December 2010.[19]Nevertheless, the market remains dominated by three companies: Korea Telecom (43.1 percent), SK Telecom (20.9 percent), and LG Telecom (16.1 percent).[20] The same firms share the country's mobile-phone service market, with 31.6 percent, 50.6 percent, and 17.8 percent, respectively.[21] All three are publicly traded companies (Korea Telecom was state-owned until privatization in 2002), but they are part of the country's *chaebol*—large, family-controlled conglomerates—which are in turn closely connected by marriage ties to the political elite.[22] This has given rise to speculation that favoritism was at play in the privatization process and in the selection of bidders for mobile-phone licenses.

One of the first priorities of the conservative government that took office in February 2008 was to restructure key regulatory institutions dealing with ICTs. The Ministry of Information and Communication (MIC) and the Korean Broadcasting Commission (KBC) were merged to create the Korea Communications Commission (KCC), tasked with overseeing both telecommunications and television broadcasting with more coherence than the previous arrangement.[23] The KCC consists of five commissioners, with the president appointing two (including the chairman) and the National Assembly choosing the remainder. Given that the first chairman is reputed to be the president's "political mentor,"[24] some observers have viewed the restructuring as an effort by the administration to establish tighter control over regulation of the ICT industry.

[18] President Lee Myung-bak's channel is located at http://www.youtube.com/user/PresidentMBLee.

[19] Korea Internet and Security Agency, "Infrastructure Statistics: ISPs," Internet Statistics Information System, 2010, http://isis.kisa.or.kr/sub01/?pageId=010302 (in Korean).

[20] Korea Communications Commission, "Broadband Subscriptions September–December 2010," Resources: Statistical Data, February 16, 2011, http://www.kcc.go.kr/user.do?mode=view&page=P02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=30824 (in Korean).

[21] Korea Communications Commission, "Wired/Wireless Subscriptions December 2010."

[22] G. M. Cho, *Study on Marriage Chains Among Korean Media Owners* (master's dissertation, Sogang University, Seoul, 2005) (in Korean); "Internet and E-Commerce Industry in South Korea," *Ecommerce Journal*, April 5, 2010, http://ecommerce-journal.com/articles/27693_internet-and-e-commerce-industry-south-korea.

[23] Jong Sung Hwang and Sang-hyun Park, "Republic of Korea," in *Digital Review of Asia Pacific 2009–2010* (London: Sage Publications, 2009), 234–240.

[24] J. N. Kang, "Who's Who Behind Lee Myung-bak: Choi See-joong the Chairman of the KCC (Appointed)," *Shindonga* (583, 2008), 48–49 (in Korean).

LIMITS ON CONTENT

As internet access has spread, online communications have become an increasingly integral part of South Korean society. Although the South Korean blogosphere is vibrant and creative, there are a number of restrictions on the free circulation of information, including content of public interest. Two types of censorship are particularly evident in South Korea: technical filtering of websites related to North Korea, and the administrative deletion of certain content on the orders of the Korea Communications Standards Commission (KCSC) and the National Election Commission (NEC).

According to testing conducted by the OpenNet Initiative in 2006 and 2008, North Korea–related content has been heavily and explicitly filtered under the provisions of the National Security Law. At least 20 websites containing North Korean propaganda or promoting reunification of the two Koreas were found to be consistently blocked by the largest ISPs.[25] By 2010, media reports indicated that the number of blocked North Korea-related sites had risen to 65.[26] A small number of gambling and Korean-language pornographic websites were found to be filtered as well.[27] The National Intelligence Service and the Korean National Police Agency can also ask the KCSC to have websites carrying pro–North Korean content blocked. The most recent example occurred in August 2010, when authorities blocked the official North Korea Twitter account, @uriminzok, within days of its launch. The justification given was that it violated the National Security Law, which classifies content that "praises, promotes, and glorifies North Korea" as "illegal information."[28]

The KCSC is an independent statutory organization. It was established in 2008 to maintain ethical standards in broadcasting and internet communications. One of its main tasks is to monitor online content for possible violations including obscenity, defamation, and threats to national security. Citizens can also submit petitions against content that they believe has violated their privacy or harmed their reputation. The KCSC then makes recommendations to bulletin board operators, or ISPs when it deems necessary, to undertake corrective measures ranging from deletion of postings to blocking of designated internet protocol (IP) addresses. Such recommendations are not legally binding in themselves. However under the Comprehensive Measures on Internet Information Protection issued in 2008, in cases of noncompliance, the KCC may step in and impose

[25] OpenNet Initiative, "Internet Filtering in South Korea in 2006–2007," http://opennet.net/studies/south-korea2007.

[26] The author has compiled the statistics from information located on the KCSC website at http://www.kocsc.or.kr/04_info/info_Communition_List.php (in Korean).

[27] OpenNet Initiative, "Country Profile—South Korea," December 26, 2010, http://opennet.net/research/profiles/south-korea.

[28] Josh Halliday, "North Korea Twitter Account Banned in South Korea," *The Guardian*, August 19, 2010, http://www.guardian.co.uk/technology/pda/2010/aug/19/north-korea-twitter-banned-south.

heavy fines on service providers.[29] Consequently, the vast majority of censorship recommendations are implemented. The KCSC process has been criticized by civil society groups for its vaguely defined standards and the wide discretionary power that this single entity possesses to determine what information should be deleted.[30]

The KCSC intermittently publishes on its website the results of its deliberations, including statistics on the corrective measures taken. From the KCSC's establishment in February 2008 to the end of 2010, 10,641 items were reportedly deleted for "disturbing social order," while 5,336 items were deleted for obscenity, 2,711 for violation of others' rights, 645 for inciting violence, and 6,171 for encouraging gambling.[31]

Among the types of content subject to potential deletion is material deemed to have "obstructed business." There have been several incidents in recent years in which content that was apparently disseminated in the public interest was nevertheless deleted. A significant example stemmed from a wave of candlelight demonstrations between May 25 and July 10, 2008. The protesters were criticizing the new conservative government for hastening an agreement to import American beef, despite public concerns over the credibility of U.S. food regulation and the danger of mad cow disease.[32] Demonstrators also began criticizing the country's three dominant, conservative newspapers—Chosun Ilbo, Joongang Ilbo, and Dong-a Ilbo, commonly referred to collectively as Chojoongdong—for being explicitly supportive of the government's actions after taking the opposite stance when the liberal government was in power. Protesters used an online bulletin board to identify companies that placed advertisements in the three dailies and threatened to boycott those that failed to withdraw their ads. The media outlets responded by pressuring the authorities to take action, and at least 58 boycott-related postings on the bulletin board were permanently deleted in July 2008 on the advice of the KCSC.[33] Boycott supporters then created a publicly accessible Google-based document in a bid to replace the bulletin board and circumvent the Korean restrictions.

In another case, the KCSC in 2007 ordered the deletion of articles posted by environmentalist Choi Byung-sung that revealed carcinogenic ingredients in cement made by particular firms. The deletion was reportedly ordered on the grounds that the articles defamed the cement companies. Choi filed a lawsuit against the KCSC's actions. On February 1, 2010, the Seoul Administrative Court ruled that the KCSC's instruction be

[29] Ha-won Jung, "Internet to Be Stripped of Anonymity," *Joongang Daily*, July 23, 2008, http://joongangdaily.joins.com/article/view.asp?aid=2892691.

[30] People's Solidarity for Participatory Democracy, "Written Statement on Freedom of Opinion and Expression of the ROK to the UNHRC," February 21, 2011, http://blog.peoplepower21.org/English/21030.

[31] The author has compiled the statistics from information located on the KCSC website at http://www.kocsc.or.kr/04_info/info_Communition_List.php (in Korean).

[32] Paul Krugman, "Bad Cow Disease," *New York Times*, June 13, 2008, http://www.nytimes.com/2008/06/13/opinion/13krugman.html.

[33] E. H. Chae, ""Delete Postings That Pressurize Advertisers in Chojoongdong", Says KCSC," *Pressian*, July 1st, 2008, http://www.pressian.com/article/article.asp?article_num=40080701194755&Section=06 (in Korean).

revoked. In addition to overturning the KCSC's directive in this instance, the ruling also set an important precedent that the commission's decisions are subject to review by administrative courts.[34]

More recently, a controversy arose after a North Korean military attack on Yeonpyeong Island in November 2010. At that time, the KCC reportedly considered the adoption of special measures under which, in "emergency situations", the KCC may directly request ISPs to delete certain content, circumventing the KCSC's deliberation. In the face of public criticism, the KCC appeared to back off from the plan.[35]

Restrictions on online expression surrounding elections are more stringent than in other democracies, and have gradually tightened since grassroots e-campaigning and citizen journalism were widely regarded as the deciding factors in the December 2002 presidential elections. Although the measures adopted have been aimed at ensuring fair electoral competition, their broad scope raises concerns about the restriction of political speech that is important for voters and candidates. Article 93 of the Public Official Election Act prohibits individual voters from distributing or displaying "an advertisement, letter of greeting, poster, photograph, document, drawing, printed matter, audio tape, video tape, or the like" during the 180 days prior to election day if it contains an endorsement of or opposition to a candidate or a political party. The NEC has interpreted this article as also applying to blog posts, user comments on news websites, and user-generated content over advanced web applications. Commissioners may demand that websites or blog-hosting services delete postings that carry such content. According to research by the OpenNet Initiative, the NEC has two divisions responsible for regulating online content related to elections: the Internet Election News Deliberation Commission, which deals with online news outlets, and the Cyber Censorship Team, which deals with user-generated content and other websites. The latter reportedly hires 1,000 part-time staff in the four months ahead of an election to monitor online content and flag violations of the election law.[36] In April 2010, the NEC issued guidelines that expanded the scope of restricted content from endorsement of candidates to endorsement of policies, thereby inhibiting the dissemination of information about key campaign issues such as environmental projects or subsidized school meals.

The aforementioned regulations, in addition to real-name registration and prosecution of bloggers, have contributed to an atmosphere of self-censorship among users, particularly on topics like North Korea. They have also led some providers and websites to institute their own registration or content monitoring policies so as to preempt censorship orders from government agencies and avoid violation of existing laws.[37]

---

[34] S. Y. Kim, ""I Thank the Toxic Cement Manufacturers", Says the Citizen Journalist Who Ignited the Debate about the Unconstitutionality of 'Internet Censorship'," *OhmyNews*, February 18, 2011, http://www.ohmynews.com/NWS_Web/view/at_pg.aspx?CNTN_CD=A0001525285 (in Korean).

[35] J. S. Kim, "Government to Pursue Unannounced Deletion of Internet Content in 'Tense Situations'," *Hankyoreh*, December 22, 2010, http://www.hani.co.kr/arti/economy/it/455022.html (in Korean).

[36] OpenNet Initiative, "Country Profile—South Korea."

[37] OpenNet Initiative, "Country Profile—South Korea."

South Koreans have enthusiastically embraced online technology to facilitate civic engagement and mobilization. As one of the first societies with widespread high-speed internet access, South Korea is home to pioneering examples of grassroots e-campaigning, such as the Nosamo internet-based voluntary association,[38] and citizen journalism initiatives such as the website OhmyNews.[39] The protests against American beef imports in 2008 marked a further development of the intersection between online and offline protest, as it featured real-time coordination and live broadcasting of large-scale demonstrations via SMS and wireless internet on personal laptops.[40]

VIOLATIONS OF USER RIGHTS

The constitution guarantees freedom of speech, the press, assembly, and association to all citizens, but it also enables restrictions, stating that "neither speech nor the press may violate the honor or rights of other persons nor undermine public morale or social ethics." South Korea has an independent judiciary and a national human rights commission that have taken decisions upholding freedom of expression. Nonetheless, a rise in criminal cases brought for online speech has generated a chilling effect, even if some of the accused have ultimately been acquitted. Following a fact-finding visit to South Korea in May 2010, the UN special rapporteur on freedom of expression, Frank La Rue, raised concerns over the government's "new and more restrictive interpretations and application of existing laws."[41]

Several laws in South Korea have been used to restrict freedom of expression in traditional media as well as for online communications. The 1948 National Security Law allows prison sentences of up to seven years for praising or expressing sympathy for the North Korean regime. In April 2010, the Ministry of Unification also issued a notice reminding users that the Act on Exchanges and Collaboration Between South and North Korea applies to online communications as well as offline encounters, and that any visit to websites or pages maintained by people in North Korea must be reported to the government in advance. Anyone failing to do so faces a fine of up to one million won (US$890).[42]

[38] Nosamo is an internet-based voluntary association Act on Exchanges and Collaboration Between South and North Korea of supporters of Roh Moo-hyun, the 16th president of South Korea, who was in office from February 2003 to February 2008. See also N. Hachigian, "Political Implications of the Information Revolution in Asia," in *The Information Revolution in Asia* (Arlington, VA: RAND, 2003), 55–91.

[39] OhmyNews is considered the inspiration for similar projects around the globe, or even "a glimpse into the future" of news media generally. D. Gillmor, *We the Media: Grassroots Journalism By the People, For the People* (Sebastopol: O'Reilly Media, 2004), 110. However, in 2010, this 10-year-old website admitted that it was less financially viable than initially thought. Eugene L. Meyer, *By The People: The Rise of Citizen Journalism* (Washington, DC: Center for International Media Assistance, December 16, 2010), http://cima.ned.org/sites/default/files/CIMA-Citizen_Journalism-Report.pdf.

[40] Sunny Lee, "Party Time at South Korea's Protest 2.0," *Asia Times*, June 13, 2008, http://www.atimes.com/atimes/Korea/JF13Dg01.html.

[41] La Rue, "Full Text of Press Statement."

[42] Ministry of Unification, "Notice on the Use of North Korean Internet Sites," News & Statements, April 8, 2010, http://www.unikorea.go.kr/CmsWeb/viewPage.req?idx=PG0000000346&boardDataId=BD00001864 51&CP0000000002

Defamation remains a criminal offense, and although prosecutions have decreased, some have occurred in recent years.

Touching more directly on online content is Article 44(7) of the Act on Promotion of Information and Communications Network Utilization and Data Protection, which lists "obstruction of business" as a punishable crime. In a high-profile case related to the above-mentioned anti-U.S. beef protests, two-dozen members of the online community established to coordinate the 2008 newspaper boycott effort were charged with obstructing business under Article 44(7). All were found guilty in the initial trial in February 2009, though nine were exonerated in an appeal in December of that year.[43]

Internet users have also faced prosecution under Article 93 of the Public Official Election Act for circulating election-related information during the restricted period before balloting. In April 2010, a 43-year-old blogger faced charges for running an informal poll about the approaching regional elections and making the results public through his Twitter account. He subsequently expressed his intention to take his case to the Constitutional Court and challenge the regulations restricting such dissemination of information.[44] During the same round of regional elections held in June 2010, Bae Ok-byeong, an education activist, was prosecuted for advocating for a free school meal program; the case was pending at year's end.[45]

A copyright law that restricts file sharing was passed in May 2009 and came into effect two months later. Often referred to as the "three-strikes rule," it allows the government to shut down an entire online bulletin board after a third warning to take down pirated content. Internet companies and civil liberties advocates have raised concerns that this is an excessive scheme which could threaten fair use and free expression.[46]

In a positive development, the Constitutional Court ruled in December 2010 that Article 47 of the Telecommunications Business Act (TBA) was unconstitutional.[47] The provision, which had been used as the basis for numerous prosecutions of bloggers, prohibited individuals from disseminating "false information" over the internet with the intent of harming the public interest, a vaguely defined term. Violations were punishable by

BO00000000033_Action=boardView&CP00000000002_BO00000000033_ViewName=board/BoardView&curNum=12 (in Korean).

[43] S. A. Gwak, "9 Netizens Not Guilty for Boycotting Chojoongdong's Advertisers," *Mediaus*, December 18, 2009, http://www.mediaus.co.kr/news/articleView.html?idxno=8890 (in Korean). There still are ongoing cases against members of the community, which is now a registered activist group called Eonsoju, a Korean acronym for Press Consumers' Rights.

[44] J. S. Ham, "First Twitter User Booked for Violation of the Election Law; Considering an Appeal to the Constitutional Court," *e-Daily*, April 30, 2010, http://www.edaily.co.kr/news/NewsRead.edy?SCD=DC16&newsid=02450166592941368&DCD=A01405&OutLnkChk=Y (in Korean).

[45] J. G. Park, "Promotion of Free School Meals Not Violation of the Election Law," *Nocut News*, February 18, 2011, http://www.nocutnews.co.kr/show.asp?idx=1722303 (in Korean).

[46] B. H. Ahn, "The New Copyright Law and 'the Three-Strikes Rule'," *Digital Times*, August 12, 2009, http://www.dt.co.kr/contents.html?article_no=2009081302011869718001 (in Korean).

[47] Song Jung-A, "S. Korean Court Rules on Internet Law," *Financial Times,* December 28, 2010, http://www.ft.com/cms/s/0/38b354a4-126d-11e0-b4c8-00144feabdc0.html.

up to five years in prison or a fine of up to 50 million won (US$44,500). The court's ruling stemmed from the case of Park Dae-sung, a popular financial blogger known as Minerva, who was arrested in January 2009 and charged with upsetting currency markets by spreading pessimistic predictions in an online discussion forum.[48] Park was detained for more than 100 days before being acquitted. The Constitutional Court ultimately found that the concept of "public interest" was so "unclear and abstract" that it failed to meet the required standard of specificity for criminal violations.[49] The decision may put an end to other investigations into "rumors" disseminated over the internet.

Anonymous communication online is significantly compromised in South Korea, given the real-name registration regime. The system has remained in place despite the national human rights commission's assertion that it "clearly qualifies as pre-censorship, restricts freedom of internet-based expression rooted in anonymity, inhibits public opinion formation, and contravenes freedom of expression."[50] While users must register their real identities before posting, they are permitted to choose pseudonyms that will appear to the public next to their comments. However, since February 2009, the portal Nate has been requiring users to have their real name displayed when leaving comments.[51] The system has encouraged some Korean users to abandon domestic services in favor of their international counterparts.[52] Mobile-phone purchase also requires users to provide their RRN if they are Korean citizens.

Regarding surveillance, individual users' personal information may be made available to the police and the prosecution upon request for investigative purposes, under Article 83(3) of the TBA. According to a recent civil society submission to the UN Human Rights Council, there were 119,280 cases of the acquisition of personal information in 2008.[53] There have also been incidents in which the authorities have failed to follow the appropriate protocol when obtaining such information, raising concerns about internet users' right to privacy. For example, prosecutors were found to have confiscated seven years' worth of e-mails sent or received by Ju Kyeong-bok, a 2008 candidate for the position of education superintendent of Seoul, during an investigation into his possible violation of the election law. In another instance, police were found to have seized e-mails and other data of human

[48] Cheon Jong-woo, "South Korea Detains Financial 'Prophet of Doom,'" *Reuters*, January 8, 2009, http://af.reuters.com/article/oddlyEnoughNews/idAFTRE50728720090108?pageNumber=1&virtualBrandChannel=0.

[49] Park Si-soo, "Law on Internet to Prosecute Rumormongers 'Unconstitutional'," *Korea Times*, December 28, 2010, http://www.koreatimes.co.kr/www/news/nation/2010/12/117_78782.html.

[50] La Rue, the UN special rapporteur, has also recommended that the system be abolished. La Rue, "Full Text of Press Statement."

[51] Reporters Without Borders, "Countries Under Surveillance: South Korea," http://en.rsf.org/surveillance-south-korea,36667.html; Developed by SK Telecom, Nate is one of the major services in the Korean cyberspace. It acquired the country's biggest social networking site Cyworld in 2003, and its instant messenger NateOn also has been more popular than international alternatives.

[52] B. G. Gu, "Legislator Choi Moon-soon Lists 5 'Backward' Regulations in the Digital Environment," *Hankyoreh*, June 24, 2010, http://www.hani.co.kr/arti/economy/it/427362.html (in Korean).

[53] People's Solidarity for Participatory Democracy, "Written Statement."

rights activist Park Rae-gun while investigating the "Yongsan tragedy"—an incident in which resistance to the forcible eviction of an area cited for demolition resulted in the deaths of five tenants and a police officer.[54] In both instances, authorities did not issue a prior notice of seizure as prescribed by the penal code.[55] In another case in 2009, television producers were charged with defaming officials from the Ministry of Agriculture in a documentary related to U.S. beef imports.[56] During the investigation, the personal e-mail accounts of the accused were searched, and certain messages were disclosed to the press in June 2009.[57] This raised objections among the legal profession as a potential violation of the law on the protection of communications secrecy and prompted one of the accused to file a lawsuit against the prosecutor's office and media outlets that carried the content of the messages. More recently, the Civil Service Ethics Division, which reports directly to the prime minister, was found to have conducted surveillance on a 56-year-old civilian, monitoring his e-mail and credit card records and secretly searching his office. The surveillance was allegedly motivated by the fact that he shared a video of a popular satire that was critical of the current president on a blog at the financial firm where he worked. This revelation was followed by other allegations in the media against the authorities' abuses of surveillance capabilities against opponents of the president. The officials involved in the surveillance scandal are still under investigation, though at least one top official had resigned by July 2010.[58]

There have been no reports of violence against bloggers by government agencies. However, online vigilantism and cyber-bullying have grown in recent years, as users, many of them teenagers, launch relentless verbal assaults over the internet against celebrities and ordinary users for comments made online or offline. In some cases, the subjects of such attacks have reportedly committed suicide because of the harassment.[59]

[54] Theresa Kim Hwa-young, "Christmas Mass for Yongshan Tragedy Victimes," *Asia News*, http://www.asianews.it/news-en/Christmas-Mass-for-Yongsan-tragedy-victims-17222.html .

[55] Ibid.

[56] They were acquitted in January 2010, but the prosecutor's office has appealed to the Supreme Court.

[57] Shin-who Kang, "Is Making Private Emails Public Justified?" *Korea Times*, June 19, 2009, http://www.koreatimes.co.kr/www/news/nation/2009/06/116_47139.html.

[58] John M. Glionna and Ju-min Park, "Agency Spied on South Korean Blogger Critical of President," *Los Angeles Times*, July 24, 2010, http://articles.latimes.com/2010/jul/24/world/la-fg-south-korea-probe-20100725.

[59] Sang-hun Choe, "South Korea Links Web Slander to Celebrity Suicides," *New York Times*, October 12, 2008, http://www.nytimes.com/2008/10/12/technology/12iht-kstar.3.16877845.html; John M. Glionna, "Cyber Bullies Reign in South Korea," *Los Angeles Times*, January 1st, 2010, http://articles.latimes.com/2010/jan/01/world/la-fg-korea-cyberthugs2-2010jan02.

THAILAND

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Not Free**
Obstacles to Access	n/a	12
Limits on Content	n/a	23
Violations of User Rights	n/a	26
Total	**n/a**	**61**

POPULATION: 68.1 million
INTERNET PENETRATION: 27 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Although Thai citizens have been posting online commentary for well over a decade,[1] internet users have played a particularly significant role in challenging the established political power structure since the military coup of September 19, 2006. Topics of discussion restricted or censored in traditional print and broadcast media are openly addressed via the internet, in particular issues related to the monarchy. Moreover, both the red-shirted United Front for Democracy Against Dictatorship (UDD) and the yellow-shirted supporters of the People's Alliance for Democracy (PAD) have utilized digital media and online resources to mobilize constituents for popular protests.[2]

This has provoked greater efforts by the government to control the free flow of information and commentary online. Over the past two years, thousands of websites have been blocked and several people prosecuted for disseminating information or views online. Internet freedom particularly deteriorated after a state of emergency was declared in April 2010; it remained in effect through to late December 2010. Ironically, the large-scale blocking of websites critical of the royal family has further deepened the politicization of the monarchy in the eyes of many Thais, while the increased content restrictions and legal harassment have contributed to greater self-censorship in online discussions. However,

[1] Phansasiri Kularb, "Communicating to the Mass on Cyberspace: Freedom of Expression and Content Regulation on the Internet," in *State and Media in Thailand During Political Transition*, ed. Chavarong Limpattanapanee and Arnaud Leveau (Bangkok: Institute de Recherche sur l'Asie du Sud-Est Contemporaine, 2007).
[2] The PAD is comprised of a grouping of royalists, business elites, and military leaders with support in the urban middle class, while the UDD generally draws its support from the north, northeast, and rural areas, among whose residents former Prime Minister Thaksin Shinawatra remains popular.

these developments have also helped inspire a burgeoning movement of politically conscious internet users, or "netizens," who favor greater protections for freedom of expression and are eager to exchange information and views about how Thailand is governed.

The first internet connection in Thailand was made in 1987 between the Asian Institute of Technology (AIT), the University of Melbourne, and the University of Tokyo. The following year, the Australian International Development Plan (IDP) assisted Prince of Songkhla University (PSU) in setting up a dial-up e-mail connection. By 1991, five universities had established internet connectivity, and by 1995, the technology was commercialized and made available to the general public.[3]

OBSTACLES TO ACCESS

According to the National Electronics and Computer Technology Center (NECTEC), the number of internet users in Thailand steadily increased from 3.5 million in 2001 to 18.3 million in 2009, or 27 percent of the country's roughly 66 million people.[4] Mobile telephony is more widespread, with over 69 million mobile-phone subscribers in 2010, and a penetration rate of 104 percent.[5] This is a marked increase from a penetration rate of about 27 percent in 2002.[6]

Internet and broadband usage continued to expand in 2010. The National Telecommunications Commission (NTC) reported that as of September 2010, Thailand had over 2.6 million broadband subscribers, representing a growth of almost 24 percent over the previous year.[7] These gains have been driven by declining prices as well as an increased demand for alternative sources of information and platforms for networking and sharing information amid the country's ongoing political crisis. The emergence of popular social-networking sites has also fueled greater internet usage. A 2009 study found that most internet users had access to high-speed internet, while approximately 10 percent used dial-up and 10 percent accessed the internet from their mobile phones.[8] Nevertheless, most complaints received by the Telecommunications Consumer Protection Institute (TCI)

[3] Sirin Palasri, Steven Huter and Zita Wenzel, *The History of the Internet in Thailand* (Eugene: University of Oregon, 1999), http://www.nsrc.org/case-studies/thailand/english/index.html.

[4] National Electronics and Computer Technology Center (NECTEC), "Internet User in Thailand," http://internet.nectec.or.th/webstats/internetuser.iir?Sec=internetuser, accessed July 3, 2010. The International Telecommunications Union (ITU) cites a similar number of 17.4 million users in 2009, "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

[5] National Telecommunications Commission (NTC), "Thailand ICT Info," December 16, 2010, http://www.ntc.or.th/TTID/.

[6] Ibid.

[7] Ibid.

[8] NECTEC, *Internet User Profile of Thailand 2009* (Bangkok: NECTEC, 2009), 52–56; National News Bureau of Thailand (NNT), "Survey Shows Growth in Internet Use," press release, January 15, 2010, http://thainews.prd.go.th/en/news.php?id=255301150043.

involve connections that prove slower than advertised by internet-service providers (ISPs).[9] High-speed internet is available in cybercafes, which are used mostly by young people to play online games.

Despite the growing usage in recent years, only 7 percent of Thai households have access to a computer, whereas color television sets can be found in 95.5 percent of households.[10] According to a 2009 study of internet users, the majority used a home or workplace connection, with only a small percentage using cybercafes.[11] The survey also found more women getting online than men. Users are concentrated in urban rather than rural areas, though the number of rural users has risen slightly in recent years.[12] Low-income groups and the elderly are also less likely to have the resources or computer literacy needed to access the internet.

Presenting another barrier to greater access, the cost of internet service in Thailand is high compared to the income of many Thais. An ADSL broadband connection costs US$20 per month,[13] while the minimum daily wage is about US$7.[14] However, the main factor behind the low penetration rates is a long-standing lack of a dedicated government effort to build up the fixed-line infrastructure and boost the development of information and communications technologies (ICTs).

Advanced web applications such as the video-sharing site YouTube, the social-networking site Facebook, the Twitter microblogging platform, and international blog-hosting services like Blogger are freely available in Thailand. Such sites have become important spaces for political expression, including messages that implicitly challenge the existing political power structure and prevalence of elite politics. Social media have also been a key channel for citizen journalists to disseminate reports on events not covered by the mainstream media, as during the civil unrest in April and May 2010.[15] YouTube, Facebook, and Twitter were all in the top 20 most visited websites in Thailand during 2010.[16] The number of Facebook users has increased exponentially in recent years, growing

[9] "Civic Sector Submitted a Complaint to TCI to Solve Problem on Telecommunications Services," Telecommunications Consumer Protection Institute (TCI), December 14, 2010, http://www.tci.or.th/newshot_detail.php?id=23#newshot (in Thai).
[10] Economist, *Pocket World in Figures: 2010 Edition* (London: Economist Newspaper Limited, 2010), 227.
[11] NECTEC, *Internet User Profile of Thailand 2009*; National News Bureau of Thailand (NNT), "Survey Shows Growth in Internet Use."
[12] Lekasina's Blog, "Internet User Profile in Thailand," blog, January 18, 2010, http://lekasina.wordpress.com/2010/01/18/internet-user-profile-in-thailand-2009/.
[13] "ADSL Internet Prices in Thailand- November 2010," Select IT, http://www.select.co.th/2010/11/adsl-internet-prices-in-thailand/, accessed February 16, 2011.
[14] "Thailand Raises Minimum Wage," Thailand Business News, December 10, 2010, http://thailand-business-news.com/economics/27852-thailand-raises-minimum-wage.
[15] Thai Netizen Network, *Internet Liberty Report 2010* (Bangkok: Thai Netizen Network, 2010).
[16] "Top Sites in Thailand," Alexa, http://www.alexa.com/topsites/countries/TH, accessed February 16, 2011.

from approximately 250,000 in January 2009 to three million in May 2010 and over six million by December 2010.[17]

Some 125 ISPs have been licensed to operate in Thailand.[18] However, the state-owned TOT, formerly the Telephone Organization of Thailand, retains the largest market share for high-speed internet services, with 41.2 percent at the end of the first quarter of 2009. Its closest competitors are two privately owned companies, True Corporation, with 37.6 percent, and TT&T, with 20.8 percent.[19]

The state-owned Communication Authority of Thailand (CAT) controls spectrum and the international internet gateway. TOT is supervised by the Ministry of Information and Communication Technology (MICT), which implements the Computer Crimes Act (CCA) of 2007 and filters restricted content. MICT oversight means that political actors are able to direct the activities of TOT and CAT, which obstructs the development of the telecommunications sector. Opening a cybercafe in Thailand involves a relatively simple registration process.

Three major mobile-phone service providers are private companies; two of them are owned by companies based in Singapore and Norway that operate under concessions from TOT and CAT. This allocation system does not promote free-market competition. The licensing process for third-generation (3G) mobile-phone service and wireless broadband has been delayed by political disputes. TOT has clashed with the NTC over the reallocation of TOT-owned spectrum, and providing 3G licenses to private mobile-phone companies, a move that it fears would cause TOT to lose significant revenue due to reduced profits from concessions. Conflicts over the creation of a new telecom regulator have also contributed to the delays.[20]

In 2004, the NTC was established as a nonpartisan regulatory body. It is generally seen as independent from the government, but is sometimes subject to political or corporate influence through patronage networks. Plans for the establishment of an independent television and radio regulator called the National Broadcasting Commission (NBC) were scuttled after the 1997 constitution was annulled during the 2006 coup, while the new constitution calls for a single entity to handle the duties of the NTC and the NBC. Legislation to that effect—an amendment of the Broadcast and Telecommunication Frequencies Allocation and Regulation Act—finally passed the parliament in late 2010, but continued disagreements among the stakeholders have further delayed the formation of and

[17] "Politics Drives Facebook Membership in Thailand Past 3 Million Mark," Asian Correspondent, May 21, 2010, http://asiancorrespondent.com/jon-russell/2010/05/21/politics-drives-facebook-membership-in-thailand-past-3-million-mark; Socialbakers, "Thailand Facebook Statistics," http://www.socialbakers.com/facebook-statistics/thailand.

[18] NTC, "List of Licensed Telecommunications Businesses," http://www.ntc.or.th/license/index.php?show=all (in Thai), accessed August 8, 2010.

[19] Sinfah Tunsarawuth and Toby Mendel, "Analysis of Computer Crime Act of Thailand," Center for Law and Democracy, May 2010, http://www.law-democracy.org/wp-content/uploads/2010/07/10.05.Thai_.Computer-Act-Analysis.pdf.

[20] Phisanu Phromchanya, "Thai Court Stalls 3G-License Auction," *Wall Street Journal*, September 16, 2010, http://online.wsj.com/article/SB10001424052748703440604575495641836172872.html#.

licensing by the merged regulator, the National Broadcast and Telecommunication Commission (NBTC). As a result, a full 3G license has not been granted, though the service is available to a limited extent via trial networks and within specific areas.[21] More generally, multiple agencies are involved with responding to reported violations of the CCA, creating confusion, overlap, and greater space for abuse of the law's vague provisions.

LIMITS ON CONTENT

Although the Thai government has been blocking some internet content since 2003, the restrictions have expanded in recent years, in terms of both the number of websites targeted and the scope of topics censored. According to a 2007 study by the OpenNet Initiative, most of the websites blocked by the authorities at the time involved pornography, online gambling, or circumvention tools. Even within those subject areas, filtering was inconsistent, with different ISPs blocking different information. Nevertheless, some politically oriented websites were found to be blocked. They included an anti-coup site (www.19sept.com) and sites related to the Patani region in the south, including the Patani Malay Human Rights Organization (www.pmhro.org). Several individual URLs selling texts critical of the monarchy were found to be blocked on the online bookseller Amazon.com.[22]

Since 2007, the number of websites blocked by the authorities has grown significantly, particularly those with content perceived as critical of the monarchy.[23] A recent academic study highlights the overall scale of, and exponential increase in, online censorship over the past three years.[24] According to the report, there have been 117 court orders to block access to nearly 75,000 URLs since 2007. On average, 690 URLs are blocked daily. In 2007, there was one court order to block two URLs. In 2008, there were 13 court orders to block 2,071 URLs. In 2009, there were 64 court orders to block 28,705 URLs, and then in 2010, there were 39 court orders to block 43,908 URLs. The research also shows that the vast majority of the websites (57,330 URLs) were blocked due to lese majeste content, while a much smaller number were blocked for material involving pornography (16,740 URLs), abortion (357 URLs), gambling (246 URLs), or other

[21] Nicole McCormick, "3G Still on Hold in Thailand," Telecom Asia, February 2, 2011, http://www.telecomasia.net/content/3g-still-hold-thailand.
[22] OpenNet Initiative, "Country Profile: Thailand," May 9, 2007, http://opennet.net/research/profiles/thailand.
[23] Freedom Against Censorship Thailand (FACT), "Thai Website Censorship Jumps by More Than 500% Since Coup!" news release, January 1, 2007, http://facthai.wordpress.com/2007/01/15/thai-website-censorship-jumps-by-more-than-500-since-coup/.
[24] Sawatree Suksri, Siriphon Kusonsinwut, and Orapin Yingyongpathana, *Situational Report on Control and Censorship of Online Media, Through the Use of Laws and the Imposition of Thai State Policies* (Bangkok: iLaw Project, 2010), http://www.boell-southeastasia.org/downloads/ilaw_report_EN.pdf [henceforth iLaw Project Report].

matters.[25] Court decisions to block URLs are reportedly made very quickly and with minimal deliberation, usually within less than a day from the application for blocking.

Online censorship intensified further after April 7, 2010, when the government declared a state of emergency and created a mechanism that allows the authorities to suddenly block—without a court order—any website considered to be publishing politically sensitive and controversial information (see below). A large number of websites focused on the opposition red shirt movement, led by the UDD, were blocked. These included individual YouTube videos, Facebook groups, and Google groups. Also filtered were less clearly partisan online news outlets or human rights groups, such as Freedom Against Censorship Thailand (FACT), the online newspaper *Prachatai*, the *Political Prisoners in Thailand* blog, and *Asia Sentinel*.[26]

International news websites like the *Economist*, the *New York Times*, the British Broadcasting Corporation (BBC), and human rights groups such as Freedom House, Human Rights Watch, Amnesty International, and Reporters Without Borders, are accessible in Thailand. However, some print editions of the *Economist* were not available because the distributors decided not to import them due to content deemed to violate lese majeste provisions. The WikiLeaks website was blocked as of the end of 2010. The organization's release of classified U.S. diplomatic cables in 2010 included explosive comments about the monarchy and the royal succession. While the leaked material was not directly accessible, Thai readers could view international media outlets with access to the files, such as Britain's *Guardian* newspaper.

Internet censorship in Thailand is carried out through judicial orders, extra-judicial blocking decisions by the executive branch, and preemptive action by ISPs and content hosts. Judicial orders are typically issued under the CCA of 2007. The law was passed by a military-appointed legislature less than a year after the 2006 coup. It groups broad content-regulation issues with more straightforward criminal activities like hacking, e-mail phishing, uploading personal content without consent, and posting obscene material. The law was opposed by a range of human rights groups on the grounds that it infringed on the right to privacy, the right to access information, and freedom of expression.[27] For example, the provisions in Articles 14 and 15 allow the prosecution of any content providers or intermediaries—such as webmasters, administrators, and managers—who are accused of posting or allowing the dissemination of content that is considered harmful to national security or public order.[28] The executive authorities, particularly the police, are left to

[25] Ibid.

[26] Pavin Chachavalpongpun, "Thailand's Massive Internet Censorship," *Asia Sentinel*, July 22, 2010, http://asiasentinel.com/index.php?option=com_content&task=view&id=2601&Itemid=164.

[27] Sarinee Achavanuntakul, "Danger! Computer Crimes Act," Fringer Blog, July 18, 2007, http://www.fringer.org/?p=259 (in Thai).

[28] Sections 14(1), 14(3), and 14(5) and Article 15 of the 2007 Computer Crimes Act pertain to crimes that "involve import to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to a third party or the public; that involve import to a computer system of any computer data related to an offense against

decide what amounts to a violation under these vaguely defined terms, and criminal courts make the final judgments. In practice, several individuals have indeed been charged under section 15 of the CCA for content posted by other users on websites or bulletin boards they hosted.[29]

Without a court order, an ISP is not necessarily required by law to comply with MICT blocking requests. However, under the April 2010 emergency declaration, which remained in effect in Bangkok and surrounding areas until December 22, 2010, top security officials held the power to shut down any website unilaterally. Thousands of websites were reportedly blocked under this extra-judicial mechanism.[30] The emergency blocking orders often encompassed a range of internet-protocol (IP) addresses, affecting a large number of lawful websites that happened to fall into the banned range.[31]

Because those providing hosting services are held responsible for comments posted by third parties, they have an interest in censoring their own sites. Self-censorship is encouraged through the work of volunteers who monitor suspicious websites and report their findings to the MICT. In October 2009 the ministry opened a call center to receive reports of dangerous websites, and in July 2010 it introduced a controversial "cyber scout" project that aims to train students as volunteer web monitors.[32] The Ministry of Justice is also conducting a cyber-scout training project designed to protect the monarchy.[33]

A case that illustrates both direct government censorship and the pressure on ISPs to preemptively censor revolves around political science scholar Professor Giles Ji Ungpakorn, who faced lese majeste charges in early 2009 for his book *A Coup for the Rich*. Professor Ungpakorn fled abroad after receiving death threats for joining the red-shirted UDD. Soon after he arrived in Britain, he used his own blog space to release the incendiary *Red Siam Manifesto*, in which he criticized the monarchy and demanded regime change.[34] In February 2009, the material was suddenly blocked by the authorities without a court order but with cooperation from ISPs. On February 13 of the same year, an MICT official sent an e-mail

---

the kingdom's security under the criminal code; that involve the dissemination or forwarding of computer data already known to be computer data [which are illegal]." The act states that "any service provider intentionally supporting or consenting to an offense…within a computer system under their control shall be subject to the same penalty as that imposed upon a person committing an offense." For an unofficial translation of the Act in English, see http://www.prachatai.com/english/node/117.

[29] iLaw Project Report pg. 13.

[30] CJ Hinke, "Thailand Now Blocking 277,610 Websites," Global Voices Advocacy, November 8, 2010, http://advocacy.globalvoicesonline.org/2010/11/08/thailand-now-blocking-256110-websites/; iLaw Project Report pg. 17.

[31] iLaw Project Report. .

[32] "Prime Minister Inaugurates 'Cyber Scout' Project; Support the MICT in building the Cyber Scout Program to Protect the Online World," Ministry of Information and Communication Technology (MICT), http://www.mict.go.th/ewt_news.php?nid=3430&filename=index (in Thai), accessed December 13, 2010; Mong Palatino, "Cyber Scout: Thailand's Internet Police?," Global Voices, December 24, 2010, http://globalvoicesonline.org/2010/12/24/cyber-scout-thailand%E2%80%99s-internet-police/.

[33] "Invitation to Participate in Scout Training Program], Ministry of Justice," http://www.justice-cyberscout.org/General/Content.aspx (in Thai), accessed December 10, 2010.

[34] Giles Ji Ungpakorn's blog is located at http://wdpress.blog.co.uk/. Access is denied in Thailand.

message to ISP executives, urging them to filter the manifesto in the name of national security.[35]

Censorship decisions, particularly those taken by the MICT, lack transparency.[36] In 2007, FACT and the Campaign for Popular Media Reform petitioned the Official Information Commission to order the release of any blocking lists, but the request was denied on the grounds that it could harm the website owners' reputations.[37]

A number of prosecutions have been initiated against internet users, and Thai authorities have begun monitoring social-networking sites in recent years, generating a chilling effect among some members of the online community. Many internet users engage in self-censorship when communicating online, even when the exchange is among friends within a closed network. Some users adjusted their use of e-mail and instant chat programs as they came to understand the ramifications of the new CCA law after its passage in 2007.

Political propagandizing and proactive state manipulation of online discussions happen occasionally but have not had a significant impact on online discourse. The military has special units tasked with creating media content to counter criticism of the monarchy, such as the Network of the Navy Quartermaster to Promote and Protect the Monarchy on the Internet.[38] Independent online news outlets sometimes face pressure from the government or private sponsors to restrict content critical of the authorities. For example, independent news site *Prachatai.com* lost a local donor for ideological reasons and consequently had difficulty sustaining itself financially.

As the number of users increases, online communication tools and resources are growing in importance for Thai citizens. Of 12,992 users included in a 2009 NECTEC survey, some 88.5 percent obtained their news from online media as well as traditional media. The most common news-related activity online was reading and participating in discussion forums or message boards, followed by reading the online versions of newspapers.[39] While many blogs and discussion sites are blocked, users can access their content with readily available circumvention software, and content producers often republish information on alternate sites. These techniques can significantly undermine the MICT's censorship efforts. After *Prachatai*'s website was blocked, for example, the number of visitors reportedly rose threefold.[40] Even a senior officer from MICT admitted at an international conference in 2010 that the blocking was not effective.[41]

[35] "MICT Asks ISPs to Block 'Red Siam,'" *Prachatai*, February 14, 2009, http://www.prachatai.com/english/news.php?id=995.
[36] For example, in seeking to collect details of blocked websites, iLaw researchers found government agency response inconsistent with several entities being unable or unwilling to provide the requested data on the number and content of censored sites.
[37] The Official Information Commission's response to the request for lists of blocked websites is available at http://www.media4democracy.com/th/images/stories/book/fact.pdf (in Thai), accessed December 13, 2010.
[38] iLaw Project Report.
[39] NECTEC, *Internet User Profile of Thailand 2009*.
[40] Private conversation with *Prachatai* director on December 17, 2010.
[41] Darren Pauli, "Our Blacklist Has Failed Us: Thai Minister," ZDNet, November 17, 2010, http://www.zdnet.com.au/our-blacklist-has-failed-us-thai-minister-339307333.htm?omnRef=http://m.blognone.com/news/20069.

Social media have become highly popular in Thailand since 2009, and the number of Facebook and Twitter users rose quickly amid the political turmoil in 2010. These platforms and the internet in general offer Thais an important alternative space to seek information and engage in political expression more freely and anonymously.[42] The red-shirt movement has used Facebook and other tools to exchange political opinions and information, and to mobilize supporters for offline actions like flash mobs and protests. Former prime minister Thaksin Shinawatra has used Twitter to send messages from exile to his supporters within Thailand. Backers of the government were also active on Facebook in 2010, with half a million signing an online petition to support the present prime minister Abhisit Vejjajiva.[43]

While internet freedom is under serious pressure, online activists are organizing to push back. For example, the *Political Prisoners in Thailand* blog provides information on lese majeste prosecutions,[44] and the Thai Netizen Network (TNN) was founded in early 2009 to uphold users' right to access, free expression, and privacy.[45] TNN makes regular public statements urging the government to respect and protect internet freedom and the rights of users.[46]

VIOLATIONS OF USER RIGHTS

The 2007 constitution, which replaced an interim charter imposed by the military government after the 2006 coup, guarantees freedom of expression. Also in 2007, the legislature passed a new Printing Act that had fewer restrictions and lighter penalties than its predecessor, the 1941 Printing and Publishing Act. However, other laws have been used to curtail free expression. These include the Internal Security Act of 2007, as well as harsh defamation and lese majeste provisions in the penal code; the latter assign penalties of up to 15 years in prison for criticism of the king, the royal family, or Buddhism.[47] In general, these provisions have been applied to online expression in much the same way as they are used against traditional media. The CCA has also been invoked to arrest internet users. This trend accelerated in 2009, when the red-shirt movement—which is tied to former prime

[42] Agence France-Presse, "Thai Political Crisis Fuels Social Media Boom," *Bangkok Post,* October 25, 2010, http://www.bangkokpost.com/news/asia/203098/thai-political-crisis-fuels-social-media-boom.

[43] See the Facebook page "Confident that more than a million Thais say no to House dissolution" at http://www.facebook.com/pages/manci-wa-khn-thiy-kein-1-lan-tx-tan-kar-yub-spha/114169001938424 (in Thai), accessed December 15, 2010.

[44] The blog is located at http://thaipoliticalprisoners.wordpress.com.

[45] The Thai Netizen Network website is located at http://www.thainetizen.org.

[46] Southeast Asian Press Alliance (SEAPA), "Thai Government Urged to Protect Netizens' Rights," news release, December 13, 2010, http://www.seapabkk.org/component/content/article/2-alerts/100382-seapa-alert-thai-government-urged-to-respect-netizens-rights.html

[47] Karin Deutsch Karlekar, ed., "Thailand," in *Freedom of the Press 2010* (New York: Freedom House, 2010), http://www.freedomhouse.org/template.cfm?page=251&year=2010.

minister Thaksin Shinawatra—mobilized in opposition to the current coalition government, led by Prime Minister Abhisit Vejjajiva.

The number of legal cases initiated against internet users since the CCA came into effect in July 2007 has increased dramatically, reaching 185 as of July 2010. Of these, 31 involved lese majeste charges (29 of them filed by the MICT or other government agency), 54 involved defamation, and six involved actions considered by the authorities to threaten national security. The remainder were related to fraud, pornography, and other commonly recognized computer crimes.[48] Most of the defendants have been ordinary Thais who were not affiliated with the red-shirts movement. At the end of 2010, the majority of the lese majeste cases were still at the initial investigation stage; however, in four cases, the courts had returned a guilty verdict. One of the first and most prominent cases centered on engineer Suwicha Thakhor, who was accused of posting clips on YouTube that attacked the royal family. He was arrested in January 2009 under penal code Article 122 and the CCA in his hometown in northeastern Nakhon Phanom province. The police also raided his other home in Bangkok, which he was accused of using as a base for spreading material that defamed the monarchy. Suwicha pleaded guilty and received a 10-year prison sentence in April 2009, but was pardoned after nearly 18 months in detention and released in June 2010.[49]

In late January 2009, a 25-year-old female user known as "Buffalo Boy" was arrested and then released on bail for the amount of two million baht (US$65,000). She was accused of posting controversial content related to the royal family on *Prachatai*'s discussion board in October 2008. In March 2009, police raided *Prachatai*'s offices and arrested Chiranuch Premchaiporn, the outlet's director and discussion-board moderator. She was accused of supporting the offending content by allowing it to remain posted for 20 days. Chiranuch was arrested once again in September 2010, this time at the airport upon returning from a conference on internet freedom. She was detained on a second charge of "defaming the royal family, and violating articles 14 and 15 of the CCA, and article 112 of the criminal code." She was released after posting a 200,000 baht (US$6500) bail,[50] and at the end of 2010 was awaiting the conclusion of her trial.

Four people were arrested between November 1 and November 18, 2009, in connection with rumors circulated the previous month about the king's health, which caused a dramatic drop in the stock market. The last of the four, 42-year-old radiologist Tassaporn Ratawongsa, was charged under Article 14 of the CCA for distributing false computer data in a manner that is likely to damage national security or cause panic.

[48] iLaw Project Report.
[49] "Thai Blogger Who Received Pardon Speaks Out," Asian Correspondent, July 1, 2010, http://asiancorrespondent.com/36769/thai-blogger-who-received-pardon-speaks-out/.
[50] Reporters Without Borders, "Prachatai Editor Released on Bail," September 24, 2010, http://en.rsf.org/thailand-news-website-editor-arrested-on-24-09-2010,38440.html.

Concerns about surveillance have led some political activists to use caution when communicating online and employ additional security and privacy tools. The CCA undermines user anonymity by requiring ISPs and webmasters to retain data logs for up to 90 days and turn it over to investigators upon request. Customers at cybercafes must present identification cards, though the smaller businesses do not always comply with this rule. Mobile-phone users are also required to register with their carriers. In practice, police reportedly need up to three days to trace the source of offensive online comments.[51] The permanent secretary for the Ministry of Information and Communication Sue Loruthai warned in the spring of 2010 that social-networking websites such as Twitter, MySpace and hi5 would be under close surveillance.[52]

In addition to legal repercussions, internet users who post controversial content can face societal harassment, termed "online witch hunts" by local observers. In a case reported in May 2010, an 18-year-old high school graduate became the subject of an online hate campaign over her alleged insult of the monarchy. The woman claimed that she was refused a place at Silpakorn University because of her Facebook postings, and expressed fears of a physical attack after her name and address were posted on public websites. She said that she faced hostility in her neighborhood as well as threatening leaflets and phone calls, and that police had refused to accept her complaint.[53] A network of users calling themselves the "Social Sanction" group has actively sought out individuals who have expressed views deemed to be disrespectful of the monarchy and launched online campaigns to vilify them. In some cases, these campaigns have sparked official investigations of the targeted individual.[54]

There have been reports of hacking attacks on online news outlets. *Prachatai* faced denial-of-service attacks many times during periods of political turmoil in 2009 and 2010 before it was officially blocked by the authorities. The attacks forced the outlet to change servers and set aside large sums to pay for extra bandwidth.

[51] Personal conversation with a senior police officer specializing in ICT crimes on March 27, 2009.
[52] Jonathan Fox, "Silenced Smiles: Freedom of Expression in Thailand," *Prachatai*, July 20, 2010, http://www.prachatai3.info/english/node/1946.
[53] Pravit Rojanaphruk, "18-Year-Old's Facebook Posting Spurs 'Hate Campaign,'" *Nation*, May 28, 2010, available on *Prachatai* at http://prachatai3.info/english/node/1864. One of the pages condemning the young woman can be found at http://www.khanpak.com/front-variety/variety-view.php?id=500
[54] iLaw Project Report pg 14.

TUNISIA

	2009	2011
INTERNET FREEDOM STATUS	Not Free	Not Free
Obstacles to Access	21	21
Limits on Content	25	28
Violations of User Rights	30	32
Total	76	81

POPULATION: 10.5 million
INTERNET PENETRATION: 34 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

EDITOR'S NOTE:

The report covers developments in Tunisia up to December 31, 2010. However, events that have occurred since the end of the coverage period have significantly altered the country's political and internet freedom landscape. In response to widespread protests against President Zine El Abidine Ben Ali and his government, the leader pledged in a speech to the nation on January 13, 2011 to, among other things, free access to the internet. Within a few hours, reports emerged that previously inaccessible websites such as the video-sharing services YouTube and Daily Motion, as well as the independent collective blog Nawaat.org, had been unblocked.

However, protests continued, and on January 14, 2011, Ben Ali fled the country. The new transitional government has generally eased restrictions on internet access. Nevertheless, the mechanism that enabled the government to block websites remains in existence. The Tunisian Internet Agency (ATI) has insisted it will only be used to block websites that "are against decency, contain violent elements, or incite hate". The ATI has also pledged to include judicial oversight in filtering decisions, though it is too early to judge whether this has been implemented.

INTRODUCTION

The internet was first launched for public use in Tunisia in 1996, and the first broadband connections were made available in 2005. Since traditional media are censored and tightly controlled by the government, the internet has been used as a comparatively open forum for airing political and social opinions, and as an alternative field for public debates on serious political issues. As the internet penetration continued to grow, the regime responded by creating an extensive online censorship and filtering system. In 2009 and especially in 2010, censorship expanded and became increasingly arbitrary. Even websites with no political or pornographic content have been censored. About 100 blogs as well as several online

applications like the photo-sharing site Flickr were blocked at least temporarily in 2010.

In an extraordinary series of events that started unfolding on December 17, 2010, an unemployed fruit vendor, Mohamed Bouazizi, set himself on fire to protest joblessness, which sparked country-wide protests and calls for political reform and greater employment opportunities. Social media sites such as Twitter, YouTube, and Facebook, as well as various blogs, have played an important role in providing independent information and analysis, spreading the protesters' demands, and showing videos of demonstrations in cities across the country. This, in turn, has resulted in the government's increased efforts to dismantle networks of online activists, hack into their social networking and blogging accounts, conduct extensive online surveillance, and disable activists' online profiles and blogs.

OBSTACLES TO ACCESS

Internet usage in Tunisia has grown rapidly in recent years, even as access remains restricted. According to the International Telecommunications Union, there were 3.5 million internet users in the country at the end of 2009, for a penetration rate of 34 percent, and reported 414,000 broadband subscriptions.[1] Although the government has actively sought to improve the country's information and communication technologies (ICTs), access is still difficult for most Tunisians due to high prices and underdeveloped infrastructure.

Tunisia has only one landline telephone provider, the state-controlled Tunisie Télécom, and every internet subscriber has to buy a landline package before choosing an internet-service provider (ISP). Tunisie Télécom's internet subscription prices range from 20 dinars (US$15) a month for a connection speed of 1 Mbps, to 50 dinars (US$38) for a connection speed of 4 megabits per second. The prices offered by other ISPs for the same speeds range from 15 to 25 dinars. Although there are no legal limits on the data capacity that ISPs supply, the bandwidth remains very low, and connectivity is highly dependent on physical proximity to the existing infrastructure.

The popularity of mobile phones is on the rise: there were over 10.7 million mobile-phone subscriptions as of June 2010, nearly double the figure from 2005.[2] Nonetheless, mobile internet connections are rarely used, since mobile-phone companies purchase internet access from existing ISPs and the cost remains beyond the reach of most Tunisians.

[1] International Telecommunications Union (ITU), "ICT Statistics 2009—Intenret," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx. More recent statistics were provided by the Tunisian Internet Agency (ATI), "Statistiques du mois de Mars 2010 sur l'Internet en Tunisie" [Statistics of March 2010 on the Internet in Tunisia], http://www.ati.tn/fr/index.php?id=90&rub=27, accessed August 2010.

[2] Ministry of Communication Technologies (Mincom), "Indicateurs et données statistiques TIC—Accés et infrastructure TIC: Nombre d'abonnements aux réseaux téléphoniques fixe et mobiles" [ICT Indicators and Statistical Data—ICT Access and Infrastructure: Number of Subscriptions to Fixed and Mobile Telephone Networks], http://www.mincom.tn/index.php?id=295&L=3, accessed August 2010.

The country's third mobile-phone company, which launched in May 2010, provides internet service through a plug-in device that enables laptops to connect to the mobile network. The device, in the form of a USB key, costs 129 dinars, and the service costs 30 dinars per month.

In 2004, the government set up an initiative to encourage widespread computer use by removing customs fees and creating the Family PC concept, according to which each family should own a personal computer. Authorities set a price ceiling for computer hardware and arranged loans at low interest rates for families to purchase the necessary equipment. The program also provided an internet subscription with every computer sold. Unfortunately, the project did not achieve the intended results, and computer prices remained prohibitively high—about 700 dinars, or three times the minimum monthly salary—even with the government incentives. Still, the number of computers per 100 inhabitants rose from 9.6 in 2008 to 12.3 in 2010, and more banks are granting Tunisians special loans to buy computers.[3] The government has also attempted to increase access to ICTs by rebuilding infrastructure to improve connectivity, and promoting competition among ISPs to lower prices.

Although many people are unable to connect at home, the government claims that universities, research centers, laboratories, and high schools have a 100 percent connectivity rate, and that 70 percent of primary schools are connected.[4] Most Tunisian users access the internet at privately owned cybercafes known as publinets.[5] According to government statistics, the number of publinets across the country reached 248 in 2009, and fell slightly to 240 in 2010. This method of access is also quite expensive for most residents, as one hour of connection may cost up to 1.50 dinars.

Tunisian users enjoy access to various internet services and applications, including free blog-hosting websites. However, a growing number of applications like the video-sharing sites Dailymotion and YouTube, and more recently Flickr and Wat TV,[6] have been systematically blocked by the government. Systems that allow voice calls over the internet are prohibited, but web-based applications like Skype and Google Talk, which provide voice and other such services, are nevertheless accessible. The social-networking site Facebook was temporarily blocked in 2008, and some groups, profiles, and video links within the application remain inaccessible. The private internet connections of some journalists,

[3] Mincom, "Indicateurs et données statistiques TIC—Accés et infrastructure TIC: Le nombre d'ordinateurs pour 100 habitants" [ICT Indicators and Statistical Data—ICT Access and Infrastructure: Number of Computers per 100 Inhabitants], http://www.mincom.tn/index.php?id=315, accessed September 22, 2010.
[4] ATI, "Statistiques du mois de Mars 2010 sur l'Internet en Tunisie."
[5] Mincom, "Indicateurs et données statistiques TIC—Accés et infrastructure TIC: Nombre de publinets" [ICT Indicators and Statistical Data—ICT Access and Infrastructure: Number of Publinets], http://www.mincom.tn/index.php?id=1062&L=3, accessed September 12, 2010.
[6] Sami Ben Gharbia, "Tunisia: Flickr, Video-Sharing Websites, Blog Aggregators and Critical Blogs Are Not Welcome," Global Voices Advocacy, April 28, 2010, http://advocacy.globalvoicesonline.org/2010/04/28/tunisia-flickr-video-sharing-websites-blogs-aggregators-and-critial-blogs-are-not-welcome/.

activists, and political bloggers are often cut, ostensibly due to "technical problems," or the speed is reduced to hamper their ability to view sites and post information. In addition, certain accounts on the Twitter microblogging service are blocked.[7]

Tunisia has 13 ISPs. Planet Tunisie, 3S Globalnet, Hexabyte, Topnet, Orange, and Tunet are privately owned, while the remaining seven are wholly or partially owned by the government and tasked with providing internet service to public institutions. The Ministry of Communication Technologies is the main government body responsible for ICTs, and its Tunisian Internet Agency (ATI) is the regulator for all internet-related activities. The law requires ISPs to obtain a license from the ministry and purchase their bandwidth from the ATI.

LIMITS ON CONTENT

Tunisia's multilayered internet censorship apparatus is one of the world's most repressive. The government employs three main techniques as part of its internet control strategy: technical filtering, postpublication censorship, and proactive manipulation. Users have increasingly complained about the expansion of this system, and the year 2010 featured an unprecedented wave of censorship that affected general blogs, photo-sharing sites, and other applications.

The government issues directives to ISPs concerning four types of content that are deemed undesirable: pornography or sexually explicit material, expressions of political opposition to the government, discussions of human rights in Tunisia (including on the websites of many nongovernmental organizations), and tools or technology that enable users to circumvent the government's controls. Directives are not issued to address specific events, since ISPs—along with online news outlets, journalists, and bloggers—are expected to be aware of the standing taboos and deal with new developments accordingly. In late 2010, the authorities also blocked access to news outlets that posted confidential cables from the U.S. Embassy, originally published by the whistle-blowing website WikiLeaks, which described deeply-rooted corruption and excessive lifestyle by President Zine El Abidine Bin Ali, his wife, and their inner circle.[8]

All of Tunisia's internet traffic flows through a single gateway controlled by the ATI, which employs SmartFilter software to limit access to specified content. URLs are blocked selectively in some cases, affecting certain pages on Wikipedia or particular videos on YouTube, for example. The authorities can also block an entire domain and the subdomains attached to it. This is the most common filtering technique, used especially to block blogs

[7] Jillian York, "Tunisia and Bahrain Block Individual Twitter Pages," Global Voices Advocacy, January 4, 2010, http://advocacy.globalvoicesonline.org/2010/01/04/tunisia-and-bahrain-block-individual-twitter-pages/.

[8] Ian Black, "WikiLeaks Cables: Tunisia Blocks Site Reporting Hatred of First Lady," Guardian.co.uk, December 7, 2010, http://www.guardian.co.uk/world/2010/dec/07/wikileaks-tunisia-first-lady.

and pages on Facebook and Twitter. The third technique targets the internet protocol (IP) addresses of websites, and has been used to block YouTube and Dailymotion. Finally, censors can employ keyword filtering, blocking access to any URL path containing a given keyword.[9] Tunisians who wish to explore the internet and visit censored websites are forced to use proxies and anonymizers. However, proxies are themselves continuously "blacklisted" by the Tunisian government, and users risk repercussions if they are caught searching for or using this technology.

Postpublication censorship can take a number of forms. Individual blog entries may be deleted, in most instances within 24 to 48 hours of their posting. In other cases, entire blogs may be shut down by service providers or through hacking. The blog *Mawtini* (My Homeland), for instance, was shut down in March 2010, just after the publication of a post denouncing the censorship of another blog, *A Tunisian Girl*.[10] Search engines filter results to exclude those that are censored or that do not favor the Tunisian government's perspective.

In addition to preventing certain content from appearing on the internet in Tunisia, the government three years ago began to proactively shape public opinion online. In 2007 it organized a small group of people to visit websites and guide discussions in a progovernment direction. This group has progressively enlarged its activities, and many blogs are created specifically to insult dissident bloggers or praise the government. Several videos promoting the idea that Tunisians enjoy political freedom and freedom of speech have been uploaded to Facebook and other websites. The authorities have also extended their control over traditional media to online news outlets by strongly encouraging them to obtain their articles from Tunisia Africa Press, the state news agency. Even independent bloggers and internet users practice varying degrees of self-censorship to avoid criminal sanctions.

The Tunisian blogosphere is still young, having taken root only in 2006, and comparatively small, with about 500 active blogs in 2010, partly due to heavy government censorship. Nevertheless, it serves as a dynamic alternative forum for the practice of free speech. Blogs have begun to play an important role in addressing issues and events that are considered to lie beyond the "red lines" observed by traditional media, such as the labor riots that took place in the Gafsa mining area in early 2008. Videos and press reports were published online on a daily basis, and a blog was created to gather all the information related to this event. In 2010, bloggers mounted a campaign against the imprisonment of a group of students after their participation in a sit-in asserting the rights of female students. Blogs covering red-line issues always find themselves censored eventually, but the deterrent effect is negligible, as bloggers simply move to another site. Some bloggers have started as many as nine blogs in an attempt to maintain their outlet for expression in the face of persistent censorship. Others have developed more creative techniques. The blog *NormalLand* discusses

[9] Sami Ben Gharbia, "A First Glimpse at the Internet Filtering in Tunisia," Global Voices Advocacy, August 18, 2010, http://advocacy.globalvoicesonline.org/2010/08/18/a-first-glimpse-on-the-internet-filtering-in-tunisia/.

[10] *Mawtini* is located at http://unsimplemec.blogspot.com; *A Tunisian Girl* is located at http://www.atunisiangirl.blogspot.com.

Tunisian politics by using a virtual country with a virtual leader, and with various government positions assigned to other Tunisian bloggers. *NormalLand* even has its own flag and national anthem modeled after the actual Tunisian versions.

Various social networking and new media sites have played an important role in the December 2010 protests, which were still ongoing at the end of the year. Activists' tweets, blogging entries, videos, and Facebook posts became key sources of information for audiences inside and outside of Tunisia, particularly given the government's tight grip on the traditional media. Bloggers, for example, wrote accounts of violence used by the police against the protestors,[11] articulated dissatisfaction felt by the Tunisian youth, and posted photos of protests from across the country. Likewise, Twitter and Facebook users posted up-to-minute developments in their home cities. And despite the official blocking of YouTube, videos of protests and the security forces' efforts to suppress them were circulated online.

VIOLATIONS OF USER RIGHTS

Tunisian law allows the government to block or censor internet content that is deemed obscene or threatening to public order, or is defined as "incitement to hate, violence, terrorism, and all forms of discrimination and bigoted behavior that violate the integrity and dignity of the human person, or are prejudicial to children and adolescents." A 2003 antiterrorism law created summary procedures for bringing terrorism suspects to trial, and stipulated that these procedures would also apply to those accused of "inciting hate or racial or religious fanaticism whatever the means used." In June 2010, the Chamber of Deputies adopted an amendment to Article 61 bis of the penal code that will punish any Tunisian who establishes deliberate contacts with foreign parties that instigate harm to Tunisia's vital interests and economic security. The existing article already punished "anyone who has undertaken, by any means whatsoever, to undermine the integrity of the Tunisian territory or has met agents of a foreign power, the purpose of the result of which is to undermine the military or diplomatic situation of Tunisia." The new law erects an added barrier against freedom of speech as well as civic activism and advocacy.

The government also uses ordinary criminal charges, such as sexual harassment and defamation, to oppress online journalists and bloggers. Between 2005 and 2007, multiple activists were prosecuted and sentenced for up to one year in prison on charges ranging from defamation to violations of public morality standards. In 2008, blogger Ziad el-Heni filed the first-ever lawsuit against the ATI, claiming that the agency practiced illegal censorship and violated his right to free expression by blocking Facebook in August of that

[11] For example, see the post on A Tunisian Girl, http://atunisiangirl.blogspot.com/2010/12/une-journee-horrible-pour-les-avocats.html.

year, but a court quickly dismissed the case.

More recently, in October 2009, the dissident journalist Taoufik Ben Brik was arrested and sentenced to six months in jail on trumped-up charges asserting that he had assaulted a woman after a traffic incident. Also that month, Zouhair Makhlouf, a human rights activist and correspondent for Assabil Online was arrested for posting a video report about environmental pollution in Nabeul, a coastal town in northeastern Tunisia. He was tried in November 2009 and sentenced to four months in jail.[12] Similarly, in another politically motivated case, online journalist Mouldi Zouabi was charged in 2010 with aggravating assault against a ruling party member. [13]

In addition to long-term imprisonment, some internet users have been arbitrarily detained and questioned. In September 2009, blogger and former political prisoner Abdallah Zouari was detained for eight hours and questioned about his contributions on the banned website Tunisia Online. Zouari spent 11 years in prison before being released in 2002, but he is constantly harassed and monitored by the police, and deprived of access to the internet.[14] Blogger and theater teacher Fatma Riahi, known online as Fatma Arabicca, was detained for five days in November 2009 and questioned about her online activities, and her computer was confiscated.[15]

The authorities have also taken measures to suppress civil society efforts to protest against online censorship. In May 2010, grassroots activists requested a permit for a peaceful rally against censorship, but on the day before the event, police detained two of the organizers who signed the request, Slim Amamou and Yassine Ayari. The two were held for more than 12 hours and forced to make videos announcing the cancelation of the rally. In August, activists against censorship decided to organize a flash mob—a sudden, unannounced public protest that is typically organized using social media. However, participants were surprised by the presence of plainclothes policemen in the secretly agreed-upon location, who forced them to leave.

Anonymity and the right to privacy are nonexistent in Tunisia. While the government does not expressly forbid anonymity and users can post anonymous comments on websites, the government has access to user information through ISPs and can trace a comment to its author. Each ISP is required to submit a list of its subscribers to the ATI on a monthly basis. Publinets are also monitored, and the managers are legally responsible for

[12] Sami Ben Gharbia, "Tunisia: Prominent Activist Arrested for Environmental Video Report Published Online," Global Voices Advocacy, October 27, 2009, http://advocacy.globalvoicesonline.org/2009/10/27/tunisia-prominent-activist-arrested-for-environmental-video-report-published-online/.

[13] "Tunisia Should Drop Charges Again Mouldi Zouabi," Committee to Protect Journalists (CPJ), December 6, 2010, http://cpj.org/2010/12/tunisia-should-drop-charges-against-mouldi-zouabi.php.

[14] Sami Ben Gharbia, "Tunisia: Journalist and Blogger Abdallah Zouari Rearrested," Global Voices Advocacy, September 17, 2009, http://advocacy.globalvoicesonline.org/2009/09/17/tunisia-journalist-and-bloggger-abdallah-zouari-rearrested/.

[15] Sami Ben Gharbia, "Tunisia: Blogger Fatma Riahi Arrested and Could Face Criminal Libel Charge," Global Voices Advocacy, November 6, 2009, http://advocacy.globalvoicesonline.org/2009/11/06/tunisia-blogger-fatma-riahi-arrested-and-could-face-criminal-libel-charge/.

customers' online activities. Owners commonly ask customers not to visit certain sites, displaying posters to remind users that pornographic and other objectionable sites are prohibited. Customers must present their identity cards to use publinet facilities, and the managers have the right to access anything saved to disk by their customers. Individuals are also required to present personal information prior to purchasing a mobile phone or SIM card, and text messaging is monitored for taboo topics in much the same way as the internet.

Online journalists and bloggers are commonly targeted with extralegal intimidation and physical violence. Sihem Bensedrine, editor in chief of the online news site Kalima, has been menaced for years with physical intimidation and smear campaigns; the site itself has been blocked since 1999. El-Heni, the journalist and blogger, has been censored more than 50 times and faces frequent intimidation and occasional physical aggression. Slim Boukhdhir, in addition to having been jailed for his writings in 2007-2008, has been repeatedly harassed by state officials. This reportedly included abuse and threats by prison guards during his seven months behind bars.

Targeted technical attacks have become a popular tool for intimidating and silencing ICT users. In 2007, Boukhdhir's blog was hacked and deleted. In 2008, an attack on Kalimatunisie.com destroyed all content on the site, forcing it to be entirely rebuilt. The administrators of Nawaat.org reported the destruction of their website several times between 2009 and 2010. E-mail hacking is also common. Accounts that have no secured access are monitored, and important information may suddenly disappear. In 2010, many cases of phishing targeting users of Google's Gmail service were reported.[16] Similarly, during the protests at the year's end, digital activists and online users reported widespread government hacking into their digital media accounts, sometimes deleting their profiles and blog entries. Apart from disrupting the networks of online activists and the free flow of information, the government's goal has been to use these methods to conduct surveillance and obtain information about the people involved in protests and digital activism.[17]

[16] Slim Amamou, "Mass Gmail Phishing in Tunisia," Global Voices Advocacy, July 5, 2010, http://advocacy.globalvoicesonline.org/2010/07/05/mass-gmail-phishing-in-tunisia/.

[17] For more information see, for example, posts by a Tunisian blogger called Astrubal found here : http://nawaat.org/portail/2011/01/03/tunisie-campagne-de-piratage-des-comptes-facebook-par-la-police-tunisienne/.

TURKEY

	2009	2011
INTERNET FREEDOM STATUS	Partly Free	Partly Free
Obstacles to Access	12	12
Limits on Content	14	16
Violations of User Rights	16	17
Total	42	45

POPULATION: 73.6 million
INTERNET PENETRATION: 36 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Internet and mobile-telephone use in Turkey has grown significantly in recent years, though access remains a challenge in some parts of the country, particularly the southeast. The government had a hands-off approach to regulation of the internet until 2001, but it has since taken considerable legal steps to limit access to certain information, including some political content. According to various estimates, there were over 5,000 blocked websites as of July 2010, spurring street demonstrations against internet censorship.[1] A related and significant threat to online freedom has been the repeated blocking of certain applications, particularly file-sharing sites like YouTube, Last.fm, and Metacafe. Over the last two years, users of these sites have filed cases with the European Court of Human Rights, after unsuccessfully appealing the ban in local courts. The YouTube block was lifted in November 2010 only after disputed videos were removed or made unavailable within the country. Despite the restrictive legal environment, the Turkish blogosphere is surprisingly vibrant and diverse. Bloggers have critiqued even sensitive government policies and sought to raise public awareness about censorship and surveillance practices, yielding at least one parliamentary inquiry into the latter.

Internet use in Turkey became popular in the mid-1990s with the introduction of home dial-up connection services. Since then, the number of dial-up users—and since 2006 the number of ADSL broadband users—has grown considerably. The government in 2003 launched the E-Transformation Turkey Project, which aims to ensure the transition to an information society.

[1] Yigal Schleifer, "Turkish Internet Users Taking It to the Streets," Eurasianet.org, http://www.eurasianet.org/node/61553.

OBSTACLES TO ACCESS

Despite an increasing penetration rate in the last few years, obstacles to internet access remain. According to the International Telecommunication Union (ITU), Turkey had approximately 26.4 million internet users in 2009, for a 35 percent penetration rate.[2] Turk Telekom announced that it reached 6.5 million broadband users in May 2010. The number of mobile-telephone subscriptions in 2009 was nearly 63 million, for a penetration rate of some 84 percent,[3] and third-generation (3G) data connections have been offered by all mobile-phone operators since June 2009. Although many people access the internet from workplaces, universities, and internet cafes, poor infrastructure—including limited telecommunication services and even lack of electricity in certain areas, especially in the eastern and southeastern regions—has a detrimental effect on citizens' ability to connect, particularly from home. High though decreasing prices, bandwidth caps, and a lack of technical literacy, especially among older Turks, also inhibit wider internet use. Bandwidth capping has become standard practice and formed part of the broadband services offered by major providers during 2010.

The population generally enjoys widespread access to internet technology, and diverse news sources are available to users. Popular social networks such as Facebook and MySpace, and other applications like Skype, can be used in Turkish. However, the government routinely blocks advanced web content and applications including video- and music-sharing sites such as YouTube, MySpace, Last.fm, Metacafe, and Dailymotion; blog-hosting sites like WordPress and Blogspot; Google groups; and the photo-sharing website Slide. In the case of YouTube alone, access was blocked roughly 20 times between March 2007 and November 2010. The block instituted in May 2008 was lifted in October 2010, only to be re-instated a few days later, then again lifted.[4] The video sharing site Vimeo was blocked in September 2010. In most instances, these large-scale shutdowns have been blunt efforts to halt the circulation of specific content that is deemed undesirable or illegal by the government. Circumvention tools are widely used to access blocked websites, and the government has not restricted their use to date.

There are 117 internet-service providers (ISPs) in Turkey, but the majority act as resellers for the dominant, partly state-owned Turk Telekom, which provides more than 95

[2] International Telecommunication Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#, accessed June 15, 2010.
[3] ITU, "ICT Statistics 2009—Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#, accessed June 15, 2010.
[4] Marc Champion, "Turkey Blocks, Unblocks YouTube," *Wall Street Journal,* November 2, 2010, http://online.wsj.com/article/SB10001424052748704462704575590420251199614.html. See also, "YouTube Removed Videos of Former Opposition Leader," Bianet.org, November 10, 2010, http://bianet.org/english/freedom-of-expression/125993-youtube-removed-videos-of-former-opposition-leader.

percent of the broadband access in the country. Liberalization of local telephony is still pending, and the delay undermines competition in the fixed-line and broadband markets. ISPs are required by law to submit an application for an "activity certificate" from the Telecommunications Communication Presidency (TIB), a regulatory body, before they can offer services. Internet cafes are also subject to regulation and registration. Those operating without an activity certificate from a local authority representing the central administration may face fines of 3,000 to 15,000 lira ($1,900 to $9,600). Mobile-phone service providers are subject to licensing through a regulatory authority, and a licensing fee set by the cabinet.

The Information and Communication Technologies Authority and the TIB, which it oversees, act as the regulators for all of these technologies and are well staffed and self-financed.[5] However, the fact that board members are government appointees is a potential threat to the authority's independence, and its decision-making process is not transparent. Nonetheless, there have been no reported instances of activity certificates being denied. TIB also oversees the application of the country's website-blocking law, and is often criticized by pressure groups for a lack of transparency. The Computer Center of Middle East Technical University has been responsible for managing domain names since 1991. Unlike in many other countries, individuals in Turkey are not permitted to register and own ".com.tr" and ".org.tr" domain names unless they own a company or a civil society organization with the same name as the requested domain.

LIMITS ON CONTENT

Government censorship of the internet is relatively common and has increased in recent years. In May 2007, the government enacted Law No. 5651, entitled "Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publication," which proscribes the responsibilities of content providers, hosting companies, mass-use providers, and ISPs.[6] Its most important provision allows the blocking of websites that contain certain types of content, including material that shows or promotes sexual exploitation and abuse of children, obscenity, prostitution, or gambling. Also targeted for blocking are websites deemed to insult Mustafa Kemal Ataturk, modern Turkey's founding father. Domestically hosted websites with proscribed content can be taken down, and those based abroad can be blocked and filtered through ISPs. A January 2010 report by the Organization for Security and Cooperation in Europe (OSCE) estimated that 3,700 websites

[5] Information and Communication Technologies Authority, http://www.tk.gov.tr/Eng/english.htm.
[6] Law No 5651 was published on the Turkish Official Gazette on 23.05.2007, No. 26030.

had been blocked as of December 2009, the number of which seems to have grown to about 5,000 by mid 2010.[7]

The procedures surrounding decisions to block websites, whether by the courts or the TIB, are nontransparent, creating significant challenges for those seeking to appeal. Judges can issue blocking orders during preliminary investigations as well as during trials. The reasoning behind court decisions is not provided in blocking notices, and the relevant rulings are not easily accessible. As a result, it is often difficult for site owners to determine why their site has been blocked and which court issued the order. The TIB's mandate includes executing judicial blocking orders, but it can also issue such orders under its own authority for certain content. Moreover, it has in some cases successfully asked content and hosting providers to remove offending items from their servers, allowing it to avoid issuing a blocking order that would affect an entire website. According to TIB statistics as of May 2009, the courts are responsible for 21 percent of blocked websites, while 79 percent are blocked administratively by the TIB. The regulator has refused to publish blocking statistics since May 2009, and legal proceedings are under way to force the release of the data under Turkey's freedom of information law.[8]

Two groups, the All Internet Association (TID) and the Turkish Informatics Association (TBD), have brought cases to the Council of State in an effort to annul as unconstitutional all the secondary regulations drawn up on the basis of Law No. 5651. The TID has particularly faulted the TIB's authority to issue administrative blocking orders without judicial involvement. The cases were still pending as of June 2010.

Although Law No. 5651 was designed to protect children from illegal and harmful internet content, its broad application to date has effectively restricted adults' access to legal content. In some instances, the courts have blocked websites for political content using other laws. For example, access to the websites of several alternative news sources such as Atilim, Özgür Gündem, Keditör, Günlük Gazetesi, and Firat News Agency are blocked indefinitely by the courts. Access to the website of Richard Dawkins a British etiologist, evolutionary biologist, and popular science writer has been blocked since September 2008 after a pro-creationist Islamist claimed that the website contents had insulted him, his work, and his religion. The website of El Mundo, a Spanish newspaper, has been banned in Turkey since April 2010 because of a single video clip deemed to be illegal.

Certain leftist and pro-Kurdish news websites are blocked consistently,[9] especially those dealing with southeastern Turkey, home to most of the country's Kurdish population. Additionally, Gabile.com and Hadigayri.com, which together form the largest online gay

[7] Yaman Akdeniz, *Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship* (Vienna: OSCE, January 2010), http://www.osce.org/documents/rfm/2010/01/42294_en.pdf. Also see "OSCE Calls on Turkey to Stop Blocking YouTube," Reuters, June 22, 2010, http://www.reuters.com/article/idUSTRE65L3MP20100622.

[8] Reporters Without Borders, "Telecom Authority Accused of Concealing Blocked Website Figures," news release, May 19, 2010, http://en.rsf.org/turkey-telecom-authority-accused-of-19-05-2010,37511.html.

[9] Yaman Akdeniz, *Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship* (Vienna: OSCE, January 2010), http://www.osce.org/documents/rfm/2010/01/42294_en.pdf.

community in Turkey with approximately 225,000 users, were also blocked for approximately seven days during 2009 by order of the TIB. Access to popular sites such as MySpace.com, Last.fm, and Justin.tv has been blocked on the basis of intellectual-property infringement.[10]

In June 2010 Turkish activists initiated a legal challenge against the government's controversial move to block Google related services, which left millions of internet users frustrated. This was a reaction to 44 IP addresses jointly used by YouTube and Google being initially blocked by the TIB, and then by the Ankara's 1st Criminal Court of Peace. The reason behind the IP address blocking was to make it even harder to access YouTube from Turkey (which had been already blocked since May 2008) but the IP blocking paralyzed access to numerous Google-related services such as Analytics, Translate, Docs, Books, Map, and Earth. However, following the unblocking of YouTube in November 2010, access to other Google services was restored.

Despite the large number of sites blocked, circumvention techniques and technologies are widely available, enabling even inexperienced users to avoid filters and blocks. Each time a new order is issued and a popular website is blocked, a large number of articles are published to instruct users on how to access the banned websites. In a sign of the extent of this phenomenon, even during the 2.5-year block, YouTube was still the eight-most-accessed site in Turkey.[11] In July 2010, Internet users organized a major protest against Internet censorship, the first of its kind. The protest gathered approximately 2,000 people in Istanbul who demanded the abolishment of Law No. 5651.[12]

Turkish users are increasingly relying on internet-based publications as a primary source of news. There is a wide range of blogs and websites on which citizens question and critique Turkish politics and leaders, including on issues that are generally viewed as politically sensitive. The majority of civil society groups maintain an online presence, and social-networking sites such as Facebook, FriendFeed, and especially the microblogging platform Twitter are used for a variety of functions, including political campaigns. Thus far, however, mobile phones and short-message service (SMS, or text messaging) technology do not seem to play a large role in social or political mobilization.

[10] In March 2010, a law professor filed a case at the European Court of Human Rights in a bid to lift the October 2009 block on Last.fm.

[11] According to Alexa, a web information company, as of August 26, 2010, http://www.alexa.com/topsites/countries/TR.

12 CyberLaw, "Turks marched against government censorship of the Internet in Istanbul," July 19, 2010, http://cyberlaw.org.uk/2010/07/19/17-temmuz-2010-internette-sansuru-protesto-etmek-icin-2000-kisi-yuruduk/

VIOLATIONS OF USER RIGHTS

The constitution includes broad protections for freedom of expression, stating that "everyone has the right to express and disseminate his thought and opinion by speech, in writing or in pictures or through other media, individually or collectively." Turkish law and court judgments are also subject to the European Convention on Human Rights and bound by the decisions of the European Court of Human Rights. While thousands of websites have been blocked under Law No. 5651, there have been no prosecutions of individuals for publication of the proscribed content. There are no laws specifically criminalizing online expression or activities like posting or downloading information, sending e-mail, or transmitting text messages. However, many provisions of the criminal code and other laws, such as the Anti-Terrorism Law, are applicable to both online and offline activity. Article 301 of the criminal code has been used against journalists who assert that genocide was committed against the Armenians in 1915, discuss the division of Cyprus, or write critically about the security forces. Book publishers, translators, and intellectuals have also faced prosecution for insulting Turkish identity. Thus far there have been no prosecutions under Article 301 for online material, but the possibility of such charges significantly contributes to self-censorship.

The constitution states that "secrecy of communication is fundamental," and users are allowed to post anonymously online. The constitution also specifies that only the judiciary can authorize interference with the freedom of communication and the right to privacy. For example, judicial permission is required for technical surveillance under the Penal Procedural Law. However, the anonymous purchase of mobile phones is not allowed, and would-be buyers need to provide official identification. The use of encryption is currently not prohibited or regulated by law, and Turkey has yet to adopt a data-protection law.

Despite the constitutional guarantees, most forms of telecommunication have been tapped and intercepted in practice.[13] Between 2008 and 2009, several surveillance scandals received widespread media attention, and it has been alleged that all communications are subject to interception by various law enforcement and security agencies, including the Gendarmerie (military police). Some reports indicate that up to 50,000 phones—both mobile and land-line—are legally tapped daily in Turkey, and 150,000 to 200,000 interception requests are made each year. During 2009 it was alleged that phone conversations involving members of the parliament, journalists, Supreme Court and other judges, and prosecutors including the chief public prosecutor were tapped.[14]

[13] For a history of interception of communications, see Faruk Bildirici, *Gizli Kulaklar Ulkesi* [The Country of Hidden Ears] (Istanbul: Iletisim, 1999); Enis Coskun, *Kuresel Gozalti: Elektronik Gizli Dinleme ve Goruntuleme* [Global Custody: Electronic Interception of Communications and Surveillance] (Ankara: Umit Yayincilik, 2000).

[14] "Başsavcı Engin dinlenmiş ve takip edilmiş" [The Chief Public Prosecutor's Calls Are Tapped]," *Radikal*, November 12, 2009.

Such actions have been challenged in court on at least one occasion. In 2008, responding to complaints lodged by the TIB, the Supreme Court of Appeals overruled a lower court's decision to grant both the Gendarmerie and the National Intelligence Agency (MIT) the authority to view countrywide data traffic retained by service providers. The court stated that "no institution can be granted such authority across the entire country, viewing all people living in the Republic of Turkey as suspects, regardless of what the purpose of such access might be."[15] Nonetheless, similar powers to access and monitor data traffic have been granted to the MIT and the National Police Department. Faced with criticism on the issue, the parliament in 2008 launched a major inquiry into illegal surveillance and interception of communications. However, the inquiry concluded in January 2009 without finding any "legal deficiencies" in the interception regime.

ISPs are not required to monitor the information that goes through their networks, nor do they have a general obligation to seek out illegal activity. However, all access providers, including internet cafe operators, are required to retain all communications (traffic) data for one year. Administrative fines of 10,000 to 50,000 lira ($6,400 to $32,200) can be imposed on access providers if they fail to comply, but to date no ISP or other provider has been prosecuted.

All mass-use providers are required to use one of the filtering programs approved by the TIB, which are published on the TIB's website. However, criteria for approval of these programs are not publicly available, and it remains unclear whether the approved programs filter websites other than the ones formally blocked by the courts and the TIB. As a result, the system could lead to systematic censorship of websites without the necessary judicial or TIB orders.

There were no reports of extralegal intimidation or harassment of bloggers or others for their online activities, though some internet content was believed to have contributed to the 2007 murder of Hrant Dink, the editor in chief of the bilingual Turkish-Armenian newspaper *Agos*. He had received several death threats via e-mail, and it was reported that his teenage killer was influenced by the writings on certain ultranationalist websites and online forums. Such sites are not covered by Law No. 5651 and have not been subject to blocking or regulation.

Unlike physical attacks, technical attacks are becoming increasingly common. On June 18, 2010 a serious denial of service (DoS) attack hit the websites of the Ministry of Transportation (http://www.ubak.gov.tr/), Information and Communication Technologies Authority (BTK) (http://www.tk.gov.tr/), and the Telecommunications Communication Presidency (TIB) (http://www.tib.gov.tr/). These websites were inaccessible for exactly 10 hours.[16] A press release sent by the hackers stated that they stopped the attack as a

[15] "Supreme Court of Appeals Overrules Gendarmerie Call Detail Access," *Today's Zaman*, June 6, 2008, http://www.todayszaman.com/tz-web/news-144038-supreme-court-of-appeals-overrules-gendarmerie-call-detail-access.html.
[16] The Register: DoS attack stuffs Turkey's internet censors, June 18, 2010, http://www.theregister.co.uk/2010/06/18/turkey_dos_attack/.

goodwill gesture, but the reason behind the attack was to protest against the unlawful blocking of access to YouTube and related IP services which crippled popular Google related services such as Maps, Docs, and Analytics from Turkey in June 2010. Turkish hackers are known to engage in minor cyberwars with their Greek and Israeli counterparts as well.

UNITED KINGDOM

	2009	2011
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access	2	1
Limits on Content	7	8
Violations of User Rights	14	16
Total	**23**	**25**

POPULATION: 62.2 million
INTERNET PENETRATION: 84 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Free

INTRODUCTION

The United Kingdom has high levels of internet penetration, and online freedom of expression is generally respected. However, both the government and private parties have presented ongoing challenges to free speech rights in connection with antiterrorism efforts, public order, and intellectual property. The biggest controversy in the past year was the adoption of the Digital Economy Act on the last day of the outgoing government in April 2010. The law allows for the blocking of websites as well as the cutting off of user accounts based on claims of intellectual-property rights violations. In a positive development, the newly elected coalition government has promised to review and repeal a number of laws that negatively affect online free expression and privacy.

The United Kingdom has been an early adopter of new information and communication technologies. The University of London was one of the first international nodes of the ARPAnet, the world's first operational packet switching network that later came to compose the global internet, and the Queen sent her first ceremonial email in 1976. Academic institutions began to connect to the network in the mid 1980s. Internet service providers (ISPs) began appearing in the late 1980s and more general commercial access was available by the early 1990s.

OBSTACLES TO ACCESS

Access to internet in the United Kingdom is widespread, and there are few practical barriers, even in rural and disadvantaged areas. The share of homes with computers has increased from 46 percent in 2000 to 76 percent in 2009, rising 6 percentage points between 2008 and 2009 alone.[1] Broadband is almost universally available, with 99.6 percent of all households capable of obtaining ADSL connections and 49 percent able to connect via cable. There is no significant difference in access between urban and rural access. As of December 2009, 73 percent of homes had internet subscriptions, and 96 percent of those used broadband.[2] The Conservative Party, which heads the coalition government elected in May 2010, has promised superfast broadband for all homes by 2017.

Those in the lowest income groups are significantly less likely to have home internet subscriptions. In addition, the share of people over 65 with an internet subscription is half that of all other age groups, but the gap has been narrowing; in the past year, two million more people obtained connections, half of them over age 50.[3]

Mobile-telephone penetration is nearly universal, with second-generation (2G) networks available in 98 percent of households and third-generation (3G) services available in around 87 percent. Some 93 percent of all households have at least one mobile phone, with 75 million in active use. Use of mobile broadband is also increasing, but it is still low at 15 percent of all households, and is most popular among younger users. Prices for telecommunications access, including mobile telephony and broadband, have continued to decline. In fact, between 2003 and 2008, cost of mobile service declined at an average annual rate of 11.8 percent to about 16 pounds (US$25) per month.[4] The price of broadband has declined 33 percent in the past five years to about 13 pounds (US$21) per month while increasing in speed from 0.6Mb to 8.2Mb/sec.[5]

The government does not place limits on the amount of bandwidth ISPs can supply, and the use of internet infrastructure is not subject to governmental control. ISPs are increasingly engaging in traffic shaping or slowdowns of certain services, such as peer-to-peer (P2P) file sharing and streaming television, while mobile providers have begun to cut back previously unlimited access packages for smart phones, reportedly because of concerns about network congestion. The Office of Communications (Ofcom), the country's

[1] Ofcom, *The Consumer Experience 2009: Research Report* (London: Ofcom, December 2009), http://stakeholders.ofcom.org.uk/market-data-research/market-data/consumer-experience-reports/ce09/.
[2] Ibid.
[3] UK Online Measurement Company, "Almost Two Million More Britons Online Than Last Year—Over Half Are Over 50," news release, June 30, 2010, http://dl.dropbox.com/u/4340062/UKOM%20PR%20290610.pdf.
[4] Ofcom, "Mobile Evolution: Ofcom's mobile sector assessment," December 2009, http://stakeholders.ofcom.org.uk/binaries/consultations/msa/statement/MSA_statement.pdf.
[5] Ofcom, "The Communications Market 2010: UK," August 2010, http://www.ofcom.org.uk/static/cmr-10/UKCM-5.92.html.

telecommunications regulator, adopted a voluntary code of practice on broadband speeds in 2008[6] and is currently holding a consultation on the subject.[7]

The United Kingdom provides a competitive market for internet access, with approximately 700 ISPs in operation, but 95 percent of users are served by five major companies. ISPs are not subject to licensing but must comply with the general conditions set by Ofcom, such as having a recognized code of practice and being a member of an alternative dispute-resolution scheme.[8] Ofcom's duties include regulating competition among communications industries, including telecommunications and wireless communications services. It is generally viewed as fair and independent in its oversight.

LIMITS ON CONTENT

There is no general law authorizing filtering or blocking of internet content. The Internet Services Providers' Association (ISPA) adopted a code of practice in January 1999 under which ISPs voluntarily agree to follow the decisions of the Internet Watch Foundation (IWF) on which content to block.[9] The IWF, a British charity funded by the industry and the European Union (EU), operates hotlines and investigates allegedly unlawful content.[10] It reportedly orders blocking of some 10,000 web pages from around the world every year, and its list contains 500 to 800 live URLs at any given time.[11] Most of the content blocked or taken down includes pornography, particularly involving children, and terrorism.

The CleanFeed filtering system, developed by British Telecom and the IWF, blocks access to any images or websites listed in the IWF database. It is estimated that 98.9 percent of all UK traffic is filtered using CleanFeed or other, less-sophisticated systems.[12] In 2009, the Home Office shelved plans to require all ISPs to implement the IWF blocking list.[13] However, an office of the Treasury Department sent out a memorandum in March 2010 stating that government bodies were prohibited from signing contracts with companies that did not agree to comply with the IWF list.[14]

---

[6] Ofcom, "Voluntary Code of Practice: Broadband Speeds," June 5, 2008, http://www.ofcom.org.uk/telecoms/ioi/copbb/copbb/.

[7] Ofcom, "Traffic Management and 'net neutrality' - A Discussion Document," http://stakeholders.ofcom.org.uk/consultations/net-neutrality/, accessed October 30, 2010.

[8] Ofcom, "The General Authorisation Regime," http://www.ofcom.org.uk/telecoms/ioi/g_a_regime/, accessed March 30, 2009.

[9] Internet Services Providers' Association, "ISPA Code of Practice," http://www.ispa.org.uk/about_us/page_16.html, accessed March 30, 2009.

[10] The Internet Watch Foundation (IWF) website is located at http://www.iwf.org.uk/.

[11] IWF, "IWF Facilitation of the Blocking Initiative," http://www.iwf.org.uk/public/page.148.htm, accessed March 30, 2009.

[12] Chris Williams, "Home Office Backs Down on Net Censorship Laws," *Register*, October 16, 2009, http://www.theregister.co.uk/2009/10/16/home_office_iwf_legislation/.

[13] Ibid.

[14] Sean O'Neill, "Government Ban on Internet Firms That Do Not Block Child Sex Sites," *Times*, March 10, 2010, http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article7055882.ece; Office of Government

The IWF's blocking and removal actions are not transparent, the blocking criteria lack clarity, and the internal appeals process is inadequate. There is no judicial or governmental oversight. The organization has issued several controversial blocking decisions in recent times. In December 2008, the IWF blocked a Wikipedia page devoted to a 1976 album by the rock band Scorpions due to an image of a nude young girl on its cover, leaving many British users temporarily unable to edit any Wikipedia content.[15] The IWF subsequently revoked its decision after protests from the Wikimedia Foundation.[16] In January 2009, the IWF blocked access to controversial images in the Internet Archive's Wayback Machine, but technical faults in ISPs' implementation of the decision resulted in inability of some users to access any of the 85 billion pages stored, including archives of the British Broadcasting Corporation (BBC) and Parliament.[17]

The Terrorism Act of 2006 allows for the takedown of terrorist material hosted in the United Kingdom.[18] ISPs reportedly take down material voluntarily when contacted by the authorities, though there are no statistics available on the practice.[19]

Users in the United Kingdom continue to enjoy wide access to free or low-cost blogging services, allowing them to express their views on the internet. Users and nongovernmental organizations also employ various forms of online communication to organize political activities, protests, and campaigns. Civil society organizations maintain a significant presence online and have used internet platforms to promote various causes. In a notable case in 2010, bloggers used Twitter to defeat a court's "super-injunction" forbidding the *Guardian* newspaper from publishing an article on the company Trafigura's dumping of toxic waste in Ivory Coast.[20] The injunction was broad enough to apply even to parliamentary debates. Bloggers also played a key role in reviewing evidence in the libel case brought against author Simon Singh by the British Chiropractic Association.[21]

Commerce, "Procurement Policy Note—Blocking Access to Web Pages Depicting Child Sexual Abuse," March 5, 2010, http://www.ogc.gov.uk/documents/PPN_05_10_Blocking_illegal_sites.pdf.

[15] "Wikipedia Child Image Censored," British Broadcasting Corporation (BBC), December 8, 2008, http://news.bbc.co.uk/2/hi/uk_news/7770456.stm; Antony Savvas, "Wikipedia Founder Considers Action Against IWF over Scorpions Image Ban," ComputerWeekly.com, December 9, 2008, http://www.computerweekly.com/Articles/2008/12/09/233807/Wikipedia-founder-considers-action-against-IWF-over-Scorpions-image.htm.

[16] Steven Musil, "Internet Watchdog U-Turns on Wikipedia Ban," ZDNet UK, December 10, 2008, http://www.zdnet.co.uk/news/networking/2008/12/10/internet-watchdog-u-turns-on-wikipedia-ban-39574751/.

[17] Cade Metz, "IWF Confirms Wayback Machine Porn Blacklisting," *Register*, January 14, 2009, http://www.theregister.co.uk/2009/01/14/iwf_details_archive_blacklisting/.

[18] Terrorism Act 2006 (c. 11), §3, available at Office of Public Sector Information, http://www.opsi.gov.uk/acts/acts2006/ukpga_20060011_en_1.

[19] Chris Williams, "Terrorism Chiefs Don't Know What They've Censored Online," *Register*, November 12, 2009, http://www.theregister.co.uk/2009/11/12/west_terror/.

[20] Steve Bell, "Trafigura Drops Bid to Gag Guardian over MP's Question," *Guardian*, October 13, 2003, http://www.guardian.co.uk/world/cartoon/2009/oct/14/trafigura-gag-steve-bell-cartoon.

[21] Robert Dougans and David Allen Green, "Virtual Veracity," *The Lawyer*, July 5, 2010, http://www.thelawyer.com/virtual-veracity/1004911.article.

VIOLATIONS OF USER RIGHTS

The United Kingdom has no written constitution or comprehensive bill of rights. The European Convention on Human Rights is incorporated into UK law through the Human Rights Act of 1998, and British courts have increasingly recognized freedom of expression and other human rights.

The Digital Economy Act was adopted in April 2010,[22] during the final parliamentary "wash-up" session—featuring limited debate—prior to Parliament's dissolution for national elections. The law gives the government the power to impose rules requiring ISPs to take "technical measures" against users who are reported (but not proven in a court or independent hearing) to be infringing copyright. The technical measures can include limiting their access speed, blocking their access to sites, and suspending their internet service altogether. ISPs will be required to track users accused of infringements, and copyright holders can apply for a court order to obtain the identification of users. Web sites that are found to have or likely to have "substantial" violations of copyright can be blocked by a court order. Ofcom has already begun developing the regulations for the law, initially only to apply to the larger ISPs.[23] There is significant concern that this will also have the effect of limiting public access though libraries, pubs, hotels, and other locations. The ISPs British Telecom and TalkTalk have begun a legal challenge of the law.[24]

The threat of libel suits has a significant chilling effect on both content producers and ISPs. English libel law is expansive in its restrictions on allegedly libelous material, and places a heavy financial and evidentiary burden on defendants.[25] The United Kingdom has implemented the EU 2002 E-Commerce Directive, which states that hosts can be held liable if they are found to have had knowledge of illicit material, including defamatory content, but failed to remove it.[26] This often results in hosting companies quickly taking down material when asked, with little inquiry as to the legality of the demand. There is also concern over "libel tourism," a practice in which overseas litigants with little or no

[22] The Digital Economy Act 2010 (c. 24), available at Office of Public Sector Information, http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_1.

[23] Ofcom, "Online Infringement of Copyright and the Digital Economy Act 2010," May 28, 2010, http://stakeholders.ofcom.org.uk/consultations/copyright-infringement/.

[24] "ISPs Take Digital Economy Act to the Courts," Out-Law.com, July 8, 2010, http://www.out-law.com/default.aspx?page=11211.

[25] Section 1, Defamation Act 1996; see Jo Glanville and Jonathan Heawood, eds., *Free Speech Is Not for Sale: The Impact of English Libel Law on Freedom of Expression* (London: Index on Censorship/English PEN, 2009), http://libelreform.org/our-report#.

[26] Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013). See *Metropolitan International Schools Ltd v. (1) Designtechnica Corporation (2) Google UK Ltd &(3) Google Inc* [2009] EWHC 1765 (QB) (search engine not liable for excerpts); *Bunt v. Tilly* [2006] EWHC 407 (QB) (ISP not liable if just provides connection); *Twentieth Century Fox Film Corporation v. Newzbin* [2010] EWHC 608 (Ch) (company that provides indexing of copyrighted files liable); *Kaschke v. Gray &Anor* [2010] EWHC 690 (QB) (host that moderates user comments liable). See also Electronic Commerce Directive (Hatred against Persons on Religious Grounds or the Grounds of Sexual Orientation) Regulations.

connection to the country exploit the ubiquity of online content to invoke plaintiff-friendly English libel laws against their critics.[27]

In the past year there has been considerable debate over the scope of the libel laws, and the current government, like its predecessor, has promised to review and amend them to better protect freedom of expression. A bill introduced in the House of Lords by Lord Lester specifically includes greater protections for ISPs to limit their liability for user-generated content.[28] The government has committed to introduce its own reform bill in 2011.

In an effort to combat terrorism, the government has taken measures against users who post or download information perceived as a security treat. For example, two students, one of whom was taking a course on the subject, were detained in 2008 under the Terrorism Act of 2000 for downloading material deemed to be terrorist in nature. In another case, a man was convicted in 2010 under the Communications Act of 2003 for using the Twitter microblogging service to express dismay at the closing of the local airport and writing that he would blow up the airport if it did not reopen within a week, which an airport manager—reading the message several days later—considered to be a threat.[29] London's Metropolitan Police Service has begun asking cybercafe owners to voluntarily monitor their users' activities as part of the antiterrorism effort, and to put up posters warning patrons not to access "inappropriate or offensive content."

Laws such as the Obscene Publications Act and the Protection of Children Act (extended in 2009) restrict possession or access to sexually oriented materials. In 2009, a man was prosecuted under the Obscene Publications Act for writing and posting online a violent sex fantasy involving the pop band Girls Aloud; the case, which ended in acquittal, had been prompted by an IWF complaint to the police.[30] Kent police in April 2010 initiated the first prosecution of a person under the law for an online chat-room conversation. The outcome of the case is expected to set an important precedent on application of the obscenity law to internet communications.[31]

There is continued concern about surveillance, as authorities have increasingly used or misused the powers granted under the Regulation of Investigatory Powers Act (RIPA).[32] The law covers the interception of communications; the acquisition of communications data,

[27] "Writ Large," *Economist*, January 8, 2009, http://www.economist.com/world/international/displaystory.cfm?story_id=12903058.
[28] Defamation Bill 2010, available at Index on Censorship, http://www.indexoncensorship.org/wp-content/uploads/2010/05/draft-bill-lester-libel.pdf.
[29] David Allen Green, "Paul Chambers: A Disgraceful and Illiberal Judgment," *Jack of Kent*, May 11, 2010, http://jackofkent.blogspot.com/2010/05/paul-chambers-disgraceful-and-illiberal.html.
[30] "Man Cleared over Girls Aloud Blog," BBC, June 29, 2009, http://news.bbc.co.uk/2/hi/uk_news/england/tyne/8124059.stm.
[31] Jane Fae Ozimek, "Mucky Private Chat Could Be Illegal Soon," *Register*, May 18, 2010, http://www.theregister.co.uk/2010/05/18/text_law_extension/.
[32] See generally the Explanatory Notes to Regulation of Investigatory Powers Act at http://www.opsi.gov.uk/acts/acts2000/en/ukpgaen_20000023_en_1, accessed January 2009.

including billing data; intrusive surveillance, such as on residential premises or in private vehicles; covert surveillance in the course of specific operations; the use of covert human intelligence sources like agents, informants, and undercover officers; and access to encrypted data. It requires that communications providers maintain interception capabilities, including systems to record internet traffic on a large scale.

RIPA allows national government agencies and nearly 500 local bodies to access communication records for a variety of reasons, from national security to tax collection. Orders for interception and access to the content of communications require approval from the home secretary or another secretary of state. In 2009, there were 525,130 requests for communications data from telephone companies (including mobile-phone service providers) and ISPs.[33] In the past few years, there have been numerous cases in which RIPA powers have been used to investigate minor violations, such as sending children to school in the wrong school district or illegal trash dumping.[34] The law has also been used against journalists to obtain their phone records and identify their sources. This has prompted orders to scale back its use.[35]

In 2009, regulations to implement the EU Data Retention Directive were adopted.[36] Under the directive, providers must retain communications data on all users for 12 months, including mobile-phone location and e-mail logs. ISPs also continue to "voluntarily" store web-access logs. Government agencies access this information through the procedures in RIPA. The Interception Modernisation Programme (IMP), a proposal to expand surveillance through deep packet inspection (DPI) and create a 2 billion pound (US$3.2 billion) central database of all communications, was hotly debated in 2009 but failed to move forward as a bill under the old government.[37] The new coalition government promised to limit the scale of surveillance conducted in the country. However, it quietly announced in late 2010 its intent to preserve the ability of various law enforcement agencies to "obtain communication data and to intercept communication within the appropriate legal framework."[38]

There has been significant public discussion surrounding the secret use of DPI by ISPs including British Telecom and Virgin in cooperation with the advertising company Phorm.[39]

---

[33] Sir Paul Kennedy, "Report of the Interception of Communications Commissioner for 2009," July 27, 2010, http://www.official-documents.gov.uk/document/hc1011/hc03/0341/0341.pdf, accessed February 15, 2011.
[34] Steve Doughty, "Councils Deploy Snooping Powers 200 Times a Week," *Daily Mail*, November 12, 2009, http://www.dailymail.co.uk/news/article-1227102/Councils-deploy-snooping-powers-200-times-week.html.
[35] Ian Grant, "UK Tightens Ripa Surveillance Rules," ComputerWeekly.com, November 4, 2009, http://www.computerweekly.com/Articles/2009/11/04/238423/UK-tightens-Ripa-surveillance-rules.htm.
[36] The Data Retention (EC Directive) Regulations 2009 (SI 2009 No. 859), April 2, 2009.
[37] London School of Economics Policy Engagement Network, *Briefing on the Interception Modernisation Programme* (London: London School of Economics and Political Science, June 2009), http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf.
[38] Tom Whitehead, "Every email and website to be stored," *Telegraph,* October 20, 2010, http://www.telegraph.co.uk/technology/news/8075563/Every-email-and-website-to-be-stored.html.
[39] Charles Arthur, "Phorm Fires Privacy Row for ISPs," *Guardian*, March 6, 2008, http://www.guardian.co.uk/technology/2008/mar/06/internet.privacy; Ian Grant, "Phorm Answers Critics at 'Town-Hall'

Providers withdrew their support for the initiative after the public outcry, and the European Commission has begun proceedings against the UK government for failing to implement the EU Telecommunications Privacy Directive.[40] Virgin is reportedly still using DPI to monitor users' sharing of copyrighted materials.[41]

There are no public restrictions on the use of encryption technologies. However, under Part 3 of RIPA, it is a crime not to disclose an encryption key upon an order from a senior policeman or a High Court judge. In 2009, the first two prosecutions under the rule yielded convictions, including that of a mentally unstable man who was not accused of committing a serious underlying crime.[42]

Meeting," ComputerWeekly.com, April 18, 2008, http://www.computerweekly.com/Articles/2008/04/21/230354/Phorm-answers-critics-at-39town-hall39-meeting.htm.

[40] European Commission, "Telecoms: Commission Steps Up UK Legal Action over Privacy and Personal Data Protection," news release, October 19, 2009, http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=5369.

[41] Chris Williams, "Virgin Media to Trial Filesharing Monitoring System," *Register*, November 26, 2009, http://www.theregister.co.uk/2009/11/26/virgin_media_detica/.

[42] Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2008–2009* (London: Stationary Office, July 2009), http://www.official-documents.gov.uk/document/hc0809/hc07/0704/0704.pdf; Chris Williams, "UK Jails Schizophrenic for Refusal to Decrypt Files," *Register*, November 24, 2009, http://www.theregister.co.uk/2009/11/24/ripa_jfl/.

UNITED STATES OF AMERICA

	2009	2011
INTERNET FREEDOM STATUS	n/a	Free
Obstacles to Access	n/a	4
Limits on Content	n/a	2
Violations of User Rights	n/a	7
Total	n/a	13

POPULATION: 309.6 million
INTERNET PENETRATION: 78 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Free

INTRODUCTION

Access to the internet in the United States remains quite free compared with the rest of the world. Users face few restrictions on their ability to access and publish content online. The courts have consistently held that federal and state constitutional prohibitions against government regulation of speech apply to material published on the internet. In addition, statutory immunity for online service providers continues to play an important role in fostering business models that permit open discourse and the free exchange of information.

However, several developments in recent years have placed the government and internet freedom advocates at odds over aspects of internet regulation as well as issues surrounding online surveillance and privacy. The United States lags behind many major industrialized countries in terms of broadband penetration, and the strength and legal viability of recent rules concerning network neutrality remain uncertain. The current administration appears committed to maintaining broad surveillance powers with the aim of combating terrorism, child pornography, and other criminal activity, and it has been reported that the government is seeking expanded authority to control the design of internet services to ensure that communications can be intercepted when necessary.

OBSTACLES TO ACCESS

Access to the internet in the United States is largely unregulated. It is controlled in practice by a small group of cable television and telephone companies that own and manage the

network infrastructure. This model has come into question in recent years amid growing concern that it is adversely affecting the economy and individuals' participation in civic life, which increasingly occurs online.[1] Observers have warned that if recent "network neutrality" regulations—discussed in greater detail below—prove too weak or are rejected by Congress or the courts, the dominant companies may decide not to continue to carry internet traffic in a content-neutral fashion.

Although the United States is one of the most connected countries in the world, it has fallen behind many other developed countries in terms of internet speed, cost, and broadband availability.[2] Approximately 78 percent of all Americans have access to the internet,[3] but only 66 percent of adults use high-speed broadband connections.[4] While the broadband penetration rate is considered high by global standards, it puts the United States significantly behind countries such as Japan, South Korea, Norway, and Sweden. Lack of high-speed internet access is particularly evident in rural areas, where the low population density makes it difficult to justify large investments in network infrastructure. In fact, broadband service is not yet available to 5 to 10 percent of U.S. residents, most of whom live in rural counties.[5]

African Americans, those living in rural areas, and those earning less than US$30,000 annually are the groups least likely to have access to the internet, though internet penetration among African Americans has been growing at significantly higher rates than in the general population. In a survey conducted by the Pew Research Center, when asked why they do not use the internet, many nonusers said they did not see the internet's relevance in their lives. They also cited factors such as availability, usability, and price as key deterrents. About 61 percent of nonusers said they would require assistance to go online if they chose to do so.[6]

[1] Mark Cooper, "The Socio-Economics of Digital Exclusion in America, 2010" (paper presented at 2010 TPRC: 38th Research Conference on Communications, Information, and Internet Policy, Arlington, Virginia, October 1–3, 2010).

[2] According to a study by the Organization for Economic Cooperation and Development (OECD), as of June 2010 the United States was ranked 9th among the OECD member countries in terms of mobile wireless broadband subscriptions per 100 inhabitants, and was ranked even lower, at 14th, on fixed-line broadband penetration. See OECD Broadband Statistics, "OECD Fixed (Wired) Broadband Subscriptions per 100 Inhabitants, by Technology, June 2010," and "OECD Terrestrial Mobile Wireless Broadband Subscriptions per 100 Inhabitants, by Technology, June 2010," http://www.oecd.org/dataoecd/21/35/39574709.xls, accessed March 4, 2011.

[3] International Telecommunications Union (ITU), "ICT Statistics 2009—Internet," available at http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx, accessed March 4, 2011.

[4] Aaron Smith, *Home Broadband 2010* (Washington, DC: Pew Internet and American Life Project, August 11, 2010), http://www.pewinternet.org/Reports/2010/Home-Broadband-2010/Summary-of-Findings.aspx; National Telecommunications Information Administration (NTIA), *Networked Nation: Broadband in America 2008* (Washington, DC: U.S. Department of Commerce, 2009).

[5] Amy Schatz, "Want Broadband? New Maps Show Options," *Digits* (blog), *Wall Street Journal*, February 17, 2011, http://blogs.wsj.com/digits/2011/02/17/want-broadband-new-map-shows-options/.

[6] Smith, *Home Broadband 2010*.

Mobile telephones, particularly models that enable internet access, have become ubiquitous in the United States. The mobile-phone penetration rate is roughly 91 percent.[7] As of mid-2010, about 38 percent of mobile-phone users reported accessing the internet on their phones, and roughly half of those users accessed the internet on a daily basis.[8] A growing number of people use their phones to check e-mail, visit social-networking sites such as Facebook, and engage in online commerce, prompting many companies to develop special applications and versions of their websites that are designed for mobile-phone viewing.

No single agency governs the internet in the United States. The Federal Communications Commission (FCC), an independent agency of the executive branch, is charged with regulating radio and television broadcasting, all interstate communications, and all international telecommunications that originate or terminate in the United States. Although the FCC is not specifically tasked with regulating the internet or internet-service providers (ISPs), it has claimed jurisdiction over some internet-related issues, such as the recent rules regarding network neutrality. Other government agencies, such as the National Telecommunications and Information Administration (NTIA), also play advisory or executive roles with respect to telecommunications, economic, and technological policies and regulations. It is incumbent upon the U.S. Congress to create laws that govern the internet and delegate regulatory authority, and government agencies such as the FCC and the NTIA must act within the bounds of congressional legislation.

Recognizing that internet penetration and connection speeds in the United States have been outpaced by those in several other developed countries, Congress has devoted funding to improving the broadband infrastructure and instructed the FCC to create a National Broadband Plan that will ensure broadband availability for all U.S. residents. Lawmakers required that this plan include a detailed strategy for reducing costs to consumers and maximizing the use of broadband to enhance health care delivery, energy efficiency, economic growth, education, and other public goods.[9] After issuing a notice of inquiry in April 2009 and weighing input from a wide variety of business, government, and civil society organizations,[10] the FCC issued its National Broadband Plan in March 2010. First among the goals is to provide at least 100 million U.S. homes with "affordable access to actual download speeds of at least 100 megabits per second and actual upload speeds of at

[7] ITU, "ICT Statistics—Mobile Cellular Subscriptions," available at http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx, accessed March 4, 2011.
[8] Aaron Smith, *Mobile Access 2010* (Washington, DC: Pew Internet and American Life Project, July 7, 2010), http://www.pewinternet.org/Reports/2010/Mobile-Access-2010/Summary-of-Findings.aspx; Amy Gahran, "Survey: U.S. Mobile Web Access Growing Fast," CNN, July 8, 2010, http://articles.cnn.com/2010-07-08/tech/mobile.internet.access.pew_1_cell-phone-users-feature-phones-mobile-internet?_s=PM:TECH.
[9] American Recovery and Reinvestment Act of 2009, H.R. 1, 111th Cong. (2009).
[10] Stephanie Condon and Marguerite Reardon, "FCC Seeks Input on National Broadband Plan," CNet News, April 8, 2009, http://news.cnet.com/8301-13578_3-10214974-38.html.

least 50 megabits per second."[11] As part of the initiative, the government has started providing subsidies to ISPs that offer satellite-based internet access in rural areas.[12]

Between 3,000 and 4,000 ISPs currently operate in the United States, although 15 of them control approximately 75 percent of the market.[13] Most of the network cables and other infrastructure are owned by large telephone and cable-television companies, such as Comcast, Time Warner, AT&T, and Verizon. Until 2005, those companies were required to grant "nondiscriminatory" access to their wire networks to other ISPs to ensure open retail-level competition and optimal service for consumers. However, in 2005, the FCC embraced an aggressive deregulation agenda and freed the network owners from the obligation to lease their lines to competing ISPs. The proponents of deregulation claimed that this step would provide more incentive for large cable and telephone companies to further develop and upgrade their networks, while opponents claimed that it would lead to fewer options for consumers, higher prices, and worse service.

One of the main policy debates surrounding the internet in the United States has to do with the concept of network neutrality, according to which network providers must treat all content, websites, and platforms equally when managing data traffic.[14] Supporters of the principle argue that without it, ISPs would be able to block certain content and applications, or give preferential treatment to some content providers for a fee. Although concerns about net neutrality began emerging in the early 2000s, the issue did not gain widespread attention until the emergence of a 2007 case involving Comcast, a cable-television company and major ISP. That year, it was revealed that the company was slowing down and blocking certain types of peer-to-peer file-sharing traffic.[15] Comcast claimed that it was forced to do so because certain high-volume users were clogging its network by repeatedly sharing large files, but its blocks were inconsistent and seemingly deceptive. For example, while engaged in peer-to-peer file sharing, a user would get a message from Comcast that looked like it came from the other computer, instructing him to stop the communication. A number of public-interest groups and academics requested that the FCC declare such blocking to be a violation of the agency's internet policy principles.[16] The FCC agreed, and Comcast appealed to the federal courts.[17] In April 2010, a federal appeals court sided with Comcast

[11] Federal Communications Commission (FCC), *National Broadband Plan: Connecting America* (Washington, DC: FCC, 2010), http://www.broadband.gov/download-plan/.

[12] Rural Utilities Service Broadband Initiatives Program, *Round Two Application Directory: Satellite, Technical Assistance, and Rural Library Broadband Grant Applications* (Washington, DC: U.S. Department of Agriculture, August 30, 2010), http://www.broadbandusa.gov/BIPportal/files/BIP_Sat_TA_RLB_App_Directory.pdf.

[13] "ISP Usage and Market Share: ISP Trends, Stats and Analysis," StatOwl.com, February 2011, http://www.statowl.com/network_isp_market_share.php.

[14] Tim Wu, "Network Neutrality FAQ," Timwu.org, http://timwu.org/network_neutrality.html, accessed March 4, 2011.

[15] Peter Svensson, "Comcast Blocks Some Internet Traffic," MSNBC, October 19, 2007, http://www.msnbc.msn.com/id/21376597/ns/technology_and_science-internet/.

[16] "Comcast Complaint," Public Knowledge, http://www.publicknowledge.org/issues/comcastcomplaint, accessed March 4, 2011.

[17] FCC, "Commission Orders Comcast to End Discriminatory Network Management Practices," news release, August 1, 2008, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-284286A1.pdf.

and overturned the FCC's ruling against the company. The decision, which came shortly after the release of the National Broadband Plan, also found that the FCC did not have the authority to regulate ISPs under the legal framework the agency had cited, challenging its ability to protect consumers on the internet.[18]

In December 2010, the FCC issued a compromise ruling on net neutrality that instructs fixed-line service providers not to block access to or unreasonably discriminate against lawful websites, applications, or devices. The rules for wireless broadband providers are much more limited, however, restricting only some types of blocking and saying nothing about discrimination. ISPs are allowed to offer tiered services at different prices under the new regulations.[19] FCC chairman Julius Genachowski claimed that the rules would protect "internet freedom and openness and promote robust innovation and investment."[20] Some civil society organizations expressed disappointment that the commission did not take a stronger stance on net neutrality that would have applied the Communications Act's "common carrier" provisions, though they agreed that the FCC operated in a free, fair, and independent manner.[21]

LIMITS ON CONTENT

Access to information on the internet is generally free from government interference. There is no government-run filtering mechanism affecting content passing over the internet or the mobile-phone network. Users with opposing viewpoints engage in a vibrant online political discourse, and face almost no legal or technical restrictions on publication or access.

Although the government does not restrict any political and social content, legal rules that apply to other spheres of life have increasingly been extended to the internet. For example, concerns over copyright violations, child pornography, protection of minors from harmful content, gambling, and financial crime have presented a strong impetus for aggressive legislative and executive action.

Advertisement, production, distribution, and possession of child pornography—on the internet and in all other media—is prohibited under federal law and can carry up to 30 years in prison. According to the Child Protection and Obscenity Enforcement Act of 1988,

[18] Comcast Corporation v. Federal Communications Commission, No. 08-1291, U.S. Court of Appeals for the District of Columbia Circuit, April 6, 2010, http://www.cadc.uscourts.gov/internet/opinions.nsf/EA10373FA9C20DEA85257807005BD63F/$file/08-1291-1238302.pdf.

[19] FCC, "Report and Order: In the Matter of Preserving the Open Internet, Broadband Industry Practices," FCC 10-201, December 21, 2010, http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db1223/FCC-10-201A1.pdf.

[20] Sara Jerome, "Genachowski on Net-neutrality: "I Reject Both Extremes," *Hillicon Valley* (blog), *The Hill*, December 20, 2010, http://thehill.com/blogs/hillicon-valley/technology/134597-genachowski-on-net-neutrality-i-reject-both-extremes.

[21] "Network Neutrality," Public Knowledge, http://www.publicknowledge.org/issues/network-neutrality, accessed March 4, 2011.

all producers of sexually explicit material must keep records proving that their models and actors are over 18 years old. In addition to prosecuting individual offenders, the Department of Justice, the Department of Homeland Security, and other law enforcement agencies can seize the domain name of an offending website after obtaining a court order.

Congress has passed several laws designed to restrict adult pornography and shield children from harmful content, such as the Child Online Protection Act of 1998 (COPA), but they were later overturned by courts due to their ambiguity and potential infringements on the First Amendment of the U.S. Constitution, which protects freedoms of speech and the press. One law that is currently in force is the Children's Internet Protection Act of 2000 (CIPA), which requires public libraries that receive certain federal government subsidies to install filtering software that prevents users from accessing "visual depictions that are obscene, child pornography, or harmful to minors." Libraries that do not receive the specified subsidies from the federal government are not obliged to comply with CIPA, and about one-third of public libraries in 2007 decided to forgo such financial support to avoid the filtering requirement.[22] Moreover, under the U.S. Supreme Court's interpretation of the law, adult users can request that the filtering be removed without having to provide a justification.[23]

Apart from clearly illegal content such as child pornography, the government in recent years has started more aggressively pursuing alleged infringements of intellectual-property rights on the internet. Over the past year alone, the Immigration and Customs Enforcement division of the Department of Homeland Security has engaged in several rounds of domain-name seizures, with targets including blogs and file-sharing sites that allegedly linked to illegal copies of music and films, and sites that sell counterfeit goods.[24] In September 2010, Senator Patrick Leahy, a Democrat from Vermont, proposed a Combating Online Infringements and Counterfeits Act (COICA), which would have authorized the attorney general to suspend any domain name that provided access to websites dedicated to copyright-infringing activities. However, the bill was criticized by some internet-freedom advocates for its potential effects on political and other speech, and it was defeated before reaching the Senate floor.

The recent activities of the antisecrecy organization WikiLeaks have touched off a serious debate about the use of the internet to publicize sensitive or classified government documents. Working with a number of traditional news outlets, WikiLeaks has published several tranches of U.S. government material that was allegedly stolen and leaked by a U.S. Army intelligence analyst, Bradley Manning. This information has included a video

[22] Charles C. McClure and Paul T. Jaeger, *Public Libraries and Internet Service Roles: Measuring and Maximizing Internet Services* (Chicago: American Library Association, 2009), 42.
[23] Bob Bocher, "Children's Internet Protection Act, CIPA: A Brief FAQ on Public Library Compliance," Wisconsin Department of Public Instruction, February 2004, updated March 11, 2010, http://dpi.state.wi.us/pld/cipafaqlite.html.
[24] Corynne McSherry, "U.S. Government Seizes 82 Websites: A Glimpse at the Draconian Future of Copyright Enforcement?" Electronic Frontier Foundation, November 29, 2010, https://www.eff.org/deeplinks/2010/11/us-government-seizes-82-websites-draconian-future.

recording from a 2007 incident in which journalists and Iraqi civilians were killed by U.S. forces (April 2010), more than 76,900 documents on the war in Afghanistan (July 2010), almost 400,000 documents about the war in Iraq (October 2010), and reams of diplomatic cables from the U.S. State Department (November 2010).

Since the release of the diplomatic cables, the WikiLeaks website has faced some unofficial, nongovernmental actions that restricted its ability to operate and obtain financial support. In late November 2010, for example, the site was removed from the data-storage service of the online commerce company Amazon, which claimed that WikiLeaks had violated its terms of service.[25] A day later, WikiLeaks' domain-name service provider, EveryDNS, ended its relationship after suffering distributed denial-of-service (DDoS) attacks by the organization's opponents.[26] The following week, the online payment service PayPal froze the account WikiLeaks had used to receive donations from the public, claiming that the group was in violation of its terms of service.[27] While each company that severed ties with WikiLeaks claimed to be acting independently and without government influence, their decisions came amid fierce public criticism of WikiLeaks by executive branch officials and prominent members of Congress.[28] Various U.S. government agencies and officials have gone so far as to instruct federal employees without proper clearance to refrain from reading the leaked cables, since they are still regarded as classified documents. The Air Force went a step further and blocked on its internal network any sites that published the cables, including those of the *New York Times* and the *Washington Post*.[29]

Although Manning, the soldier accused of passing the classified information to WikiLeaks, is facing a military prosecution that could end with a sentence of life in prison, the government to date has not filed charges over the actual publication of the leaked material, nor has it sought to block access to the information or ban publication of future leaks.

A communications start-up community is thriving in the United States, despite the recent economic recession, and such innovators and entrepreneurs regularly offer new technological tools at no cost to the public. Popular web applications like the video-sharing site YouTube, the social-networking site Facebook, the Twitter microblogging service, and international blog-hosting services are all freely available. The internet plays a significant role in civic activism in the United States, and the growth of the blogosphere and citizen

[25] Geoffrey A. Fowler, "Amazon Says WikiLeaks Violated Terms of Service," *Wall Street Journal*, December 3, 2010, http://online.wsj.com/article/SB10001424052748703377504575651321402763304.html.
[26] Kevin Poulsen, "WikiLeaks Attacks Reveal Surprising, Avoidable Vulnerabilities," *Wired*, December 3, 2010, http://www.wired.com/threatlevel/2010/12/wikileaks-domain/.
[27] Kevin Poulsen, "PayPal Freezes WikiLeaks Account," *Wired*, December 4, 2010, http://www.wired.com/threatlevel/2010/12/paypal-wikileaks/.
[28] Ewen MacAskill, "WikiLeaks Website Pulled by Amazon After US Political Pressure," *Guardian*, December 2, 2010, http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon.
[29] Eric Schmitt, "Air Force Blocks Sites that Posted Secret Cables," *New York Times*, December 14, 2010, http://www.nytimes.com/2010/12/15/us/15wiki.html.

journalism has changed the ways in which many people receive news. Blogs and electronic media outlets reporting from various points on the political spectrum now have greater readership than most printed periodicals. Nearly all nongovernmental organizations and causes have a presence on the internet and use it for advocacy and social mobilization. E-mail campaigns, online petitions, and YouTube videos have been instrumental in organizing protests, lobbying government bodies, and putting a spotlight on issues ranging from environmental degradation to hate crimes.[30]

The internet has also profoundly influenced political campaigning and fundraising. Until recently, most election campaigns relied on large donations from a limited pool of wealthy contributors. However, the success of current U.S. president Barack Obama's 2008 campaign, which was propelled by millions of small, online contributions, demonstrated the efficacy of the internet in mobilizing mass political support. Obama's election team was able to raise over half a billion dollars in internet-based donations, with an average donation of about $80.[31] In addition, the campaign's use of e-mail, social-networking tools, and online videos was watched and eventually emulated by political operatives in the United States and around the world.

VIOLATIONS OF USER RIGHTS

The U.S. Constitution includes strong protections for free speech and freedom of the press. In 1997, the U.S. Supreme Court applied established standards on those rights to the internet, and the lower courts have consistently enforced them. Two federal laws also provide significant protections for online speech: Section 230 of the Communications Act of 1934 (as amended by the Telecommunications Act of 1996) provides immunity for ISPs and online platforms such as YouTube and Facebook that carry content created by third parties, and the Digital Millennium Copyright Act (DMCA) requires copyright owners to notify intermediaries to have allegedly infringing material removed. These statutes effectively enable companies to develop internet applications and websites without fear that they will be held liable for content posted by users.

The U.S. government generally does not prosecute individuals for posting information on the internet. As of the end of December 2010, it had taken no decisive action against either WikiLeaks or its founder, Julian Assange, an Australian citizen. However, Attorney General Eric Holder has stated that his office is looking into whether

[30] See for example the Care2 "Keep Sewage Out of Our Rivers!" petition at http://www.thepetitionsite.com/takeaction/200/475/680/, and Steve Williams, "President Obama Signs Hate Crimes Bill—Thank You to the 25,000 Care2 Members That Helped It Reach His Desk!" Care2, October 28, 2009, http://www.care2.com/causes/civil-rights/blog/25-000-care2-members-help-secure-presidents-signature-on-hate-crimes-bill/.

[31] Jose Antonio Vargas, "Obama Raised Half a Billion Online," *44* (blog), *Washington Post*, November 20, 2008, http://voices.washingtonpost.com/44/2008/11/obama-raised-half-a-billion-on.html.

any such charges would be appropriate.[32] Many analysts argue that given the applicable laws and legal precedents, the government is unlikely to prosecute Assange or WikiLeaks for merely publishing leaked information. But some reports have suggested that federal officials are attempting to build a case that WikiLeaks played a conspiratorial role in the Army analyst's unauthorized downloading of classified documents from U.S. military computers, or in his subsequent transmission of the material to WikiLeaks.[33]

There are no legal restrictions on user anonymity on the internet, and constitutional precedents protect the right to anonymous speech in many contexts. There are also state laws that stipulate journalists' right to withhold the identities of anonymous sources, and at least one such law has been found to apply to bloggers.[34] In June 2010, the Obama administration released plans for a National Strategy for Trusted Identities in Cyberspace (NSTIC). The stated goal of the effort is to ensure the creation of an "identity ecosystem" in which internet users and organizations can more completely trust one another's identities and systems when carrying out online transactions.[35] While the plan does not include mandatory registration, some commentators have expressed their concerns about its potential effects on anonymous speech.[36]

The contents of internet communications are generally protected from government intrusion by constitutional rules against unreasonable searches and seizures,[37] but law enforcement and intelligence agencies can access such information with varying degrees of judicial oversight as part of criminal or national security investigations. In criminal probes, law enforcement authorities can obtain court orders to monitor specified internet communications if they persuade a judge that there is probable cause to believe that a crime has been or will be committed. The Communications Assistance for Law Enforcement Act (CALEA) requires telephone companies, broadband carriers, and interconnected Voice over Internet Protocol (VoIP) providers to design their systems so that communications can be easily intercepted when government agencies have the legal authority to do so,[38] and some in the Obama administration suggested in late 2010 that the law could be expanded to

[32] "Holder: Wikileaks Probe 'Serious Investigation,'" KTVU San Francisco, December 10, 2010, http://www.ktvu.com/news/26092558/detail.html.
[33] Charlie Savage, "U.S. Weighs Prosecution of Wikileaks Founder, but Legal Scholar Warns of Steep Hurdles," *New York Times*, December 1, 2010, http://www.nytimes.com/2010/12/02/world/02legal.html.
[34] "Apple v. Does," Electronic Frontier Foundation, http://www.eff.org/cases/apple-v-does, accessed March 4, 2011.
[35] A site created to foster discussion on the proposed strategy can be found at http://www.nstic.us/.
[36] Jay Stanley, "Don't Put Your Trust in 'Trusted Identities,'" *Blog of Rights*, American Civil Liberties Union, January 7, 2011, http://www.aclu.org/blog/technology-and-liberty/dont-put-your-trust-trusted-identities; Jim Dempsey, "New Urban Myth: The Internet ID Scare," *Policy Beta* (blog), Center for Democracy and Technology, January 11, 2011, http://www.cdt.org/blogs/jim-dempsey/new-urban-myth-internet-id-scare.
[37] Paul Ohm, "Court Rules Email Protected by Fourth Amendment," *Paul Ohm's Blog*, *Freedom to Tinker*, December 14, 2010, http://www.freedom-to-tinker.com/blog/paul/court-rules-email-protected-fourth-amendment.
[38] The FCC does not classify Skype as an "interconnected VoIP."

permit increased access to online communications tools such as Gmail, Skype, and Facebook.[39]

Following the terrorist attacks of September 11, 2001, Congress passed the USA PATRIOT Act, which broadly expanded the government's surveillance and investigative powers in cases involving terrorism. Among other things, the law requires ISPs to provide more detailed information about the internet activities of terrorism suspects—including their browsing history—with less judicial oversight and, in some cases, without probable cause. In February 2010, three expiring provisions of the USA PATRIOT Act were renewed for an additional year, including the government's broad authority to conduct roving wiretaps of unidentified or "John Doe" targets, to wiretap "lone wolf" suspects who have no known connections to terrorist networks, and to secretly access a wide range of private business records without warrants under Section 215.[40]

[39] Charlie Savage, "U.S. Tries to Make it Easier to Wiretap the Internet," *New York Times*, September 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=1.
[40] "Patriot Act Excesses," *New York Times*, October 7, 2009, http://www.nytimes.com/2009/10/08/opinion/08thu1.html.

VENEZUELA

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Partly Free**
Obstacles to Access	n/a	15
Limits on Content	n/a	13
Violations of User Rights	n/a	18
Total	**n/a**	**46**

POPULATION: 28.8 million
INTERNET PENETRATION: 35 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

The Venezuelan constitution guarantees freedom of expression, and the government regards access to the internet as a priority for the country's economic and social development.[1] Internet access has increased dramatically over the past decade, and the country has emerged as a leader in the use of social media platforms. In the context of growing restrictions on broadcast outlets and severe political polarization in the traditional media overall,[2] new media—especially blogs, the social-networking site Facebook, and the microblogging platform Twitter—have become important spaces for the diffusion of information and opinions on political and social topics. As government opponents have mobilized via these platforms, the authorities have taken measures in recent years to restrict online content and have hinted at future efforts to contain the influence of new media.

In March 2010, President Hugo Chavez declared that the internet could not be "a free thing where you do and say whatever you want."[3] Despite such warnings, the Venezuelan authorities do not engage in systematic filtering or large-scale arrests of bloggers. Nevertheless, there have been periodic interruptions of access to opposition or independent websites, efforts to intimidate websites to censor the comments of their users,

[1] Presidential Decree No. 825 (May 2000) designates access to and use of the internet as political priorities for the development of the country. See *Gaceta Oficial* no. 36.955, May 22, 2000, http://www.tsj.gov.ve/gaceta/mayo/220500/220500-36955-01.html (in Spanish).
[2] M. Bisbal, ed., *Hegemonía y control comunicacional* [Hegemony and Communications Control] (Caracas: Editorial Alfa, 2009), 270 (in Spanish).
[3] *Hugo Chávez: "Internet No Puede Ser Libre"* [Hugo Chávez: "Internet Cannot Be Free"] (YouTube, March 20, 2010), 1 min., 46 sec., http://www.youtube.com/watch?v=s37YZ0bbblk&feature=related (in Spanish).

and several prosecutions launched against users for information posted on Twitter. Perhaps the most worrying recent development for online freedoms in Venezuela was the passage in December 2010 of laws increasing state control over telecommunications networks and laying the foundation for website managers and service providers to be required to censor users commenting on the platforms they host.

The internet arrived in Venezuela in 1992, but its popularization began in 1996, when the first commercial internet-service providers (ISPs) were granted licenses by the National Telecommunications Committee (Conatel).[4] The 1999 constitution obliges the state to provide the public with access to new information and communication technologies (ICTs),[5] and the 2000 Organic Law of Telecommunications enables private companies to enter the market.[6]

OBSTACLES TO ACCESS

Over the past 10 years, partly due to government investment, internet penetration has grown rapidly, increasing from under 4 percent in 2000 to 34.67 percent—or almost 10 million users—by late 2010, according to statistics provided by Conatel. Recent years have seen a significant shift from dial-up to broadband, and by 2010, over 90 percent of the nearly 2.5 million internet subscriptions were broadband.[7] Despite the prevalence of broadband connections, such services are slower and more expensive than in other countries in Latin America.[8] The state-owned telecommunications firm National Telephone Company of Venezuela (CANTV) offers relatively low prices, but its connections are slow, and the company's dominant position stifles competition. Nationally, the average connection speed is less than 1 Mbps,[9] with a cost of approximately US$30-45 per month.[10] According to a

[4] United Nations Development Programme (UNDP), *Las Tecnologías de Información y Comunicación al Servicio del Desarrollo* [Information and Communication Technologies for Development] (Caracas: UNDP, 2002), 249 (in Spanish).
[5] See Articles 108 and 110 of the constitution, available at http://www.tsj.gov.ve/legislacion/constitucion1999.htm (in Spanish).
[6] In July 2008, a plan to reform the law was leaked to the press. Due to the opposition it garnered, the measure was not introduced in the National Assembly. The proposed modifications included the establishment of a single node for internet service, provided by Conatel, which would have constituted a risk to the neutrality of internet service and management.
[7] Conatel, *Estadísticas preliminares del sector Telecomunicaciones al cierre del III trimestre de 2010* [Statistics from the Telecommunications Sector at the end of the Third Trimester of 2010] (Caracas: Conatel, 2010), http://www.conatel.gob.ve/files/Indicadores/indicadores2010/presentacion_a_publicar_III_trim_20102.pdf (in Spanish).
[8] BuddeComm, "Venezuela—Broadband & Broadcasting Market—Overview, Statistics & Forecasts," https://www.budde.com.au/Research/Venezuela-Broadband-Broadcasting-Market-Overview-Statistics-Forecasts.html?r=51, accessed August 12, 2010.
[9] Speedtest.net, "World Speedtest.net Results," http://www.speedtest.net/global.php#0, accessed August 12, 2010.
[10] In Venezuela, foreign-exchange controls have been in place since 2003. In January 2010, a variable rate of 2.60 bolivares per dollar was decreed for preferential imports such as food and pharmaceutical drugs, a rate of 4.30 was decreed for sectors including telecommunications, and another rate of approximately 5.30 bolivares per dollar, which one could obtain through relatively strict auctions, was applied to automobiles. Calculating the minimum wage at 2.60 bolivares per dollar is, according to many economists, somewhat illusory.

recent study, just over half of all users connect to the internet via cybercafes, while an additional third use home connections.[11] About 53 percent of users are male, and 43 percent are minors.[12] In Caracas, the capital, WiMAX internet service is available, but only as a trial program with about 5,000 users.[13]

The most significant obstacles to internet access in Venezuela are lack of service availability, low computer literacy, and the high cost of a connection and necessary equipment. Of the Venezuelans who have difficulty accessing the internet, two thirds are disadvantaged by low income, geographic isolation in rural zones, disabilities, or old age. Internet penetration in the lowest income bracket, where the largest proportion of the population is concentrated, is below the national average.[14] In a study of Venezuelans who do not use the internet, one third cited the lack of sufficient knowledge as the primary reason, while an additional third reported the lack of a connection or a computer in their home; 8.8 percent pointed to high costs.[15]

There are about seven million landline telephone subscribers, the equivalent of about 25 percent of the population.[16] By contrast, mobile phones are almost ubiquitous, with a penetration rate of 101.50 percent,[17] although some areas between towns experience limited coverage. Venezuela is a regional leader in text messaging (short-message service, or SMS) with some 21.4 million text messages sent during the last four months of 2010.[18] There is a growing contingent of people subscribing to mobile internet services, particularly

[11] "Venezuela Internet: Sub-sector Update," Economist Intelligence Unit (EIU), November 6, 2009, http://www.eiu.com/index.asp?layout=ib3PrintArticle&article_id=1845094769&printer=printer.

[12] Carlos Jiménez, *Números y Palabras, Usos y Penetración de Internet en Venezuela* [Numbers and Words, Uses and Internet Penetration in Venezuela] (Caracas: Tendencias Digitales, May 2009), slides, http://www.slideshare.net/Tendencias_Digitales/nmeros-y-palabras-presentacin-sobre-usos-y-penetracin-de-internet-en-venezuela?type=presentation (in Spanish).

[13] "Movilmax lanzará servicio de VoIP sobre WiMAX para aumentar número de usuarios" [Movilmax Launches VoIP over MiMAX Service to Increase the Number of Users], TeleSemana.com, October 9, 2008, http://www.telesemana.com/entrevistas/detalle.php?id=60 (in Spanish).

[14] Bevilacqua, "Carlos Jiménez: 'En 2012 más de la mitad de los venezolanos estarán conectados a la red.'"

[15] Carlos Jiménez, *Estadísticas y Tendencias de Internet en Venezuela* [Statistics and Trends of the Internet in Venezuela] (Caracas: Tendencias Digitales, 2010), slides, http://www.slideshare.net/Tendencias_Digitales/estadsticas-y-tendencias-de-internet-en-venezuela-vp (in Spanish).

[16] Conatel, *Estadísticas preliminares del sector Telecomunicaciones al cierre del III trimestre de 2010* [Statistics from the Telecommunications Sector at the end of the Third Trimester of 2010]

[17] Ibid. The elevated proportion of prepaid service users in Latin America and the Caribbean has resulted in some double counting, due to multiple payments and inactive accounts. See International Telecommunication Union (ITU), *Perfiles Estadísticos de la Sociedad de la Información: Región de América* [Statistical Profiles of the Information Society: Americas Region] (Geneva: ITU, 2009), http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-RPM.AM-2009-E09-R1-PDF-S.pdf (in Spanish).

[18] Conatel, *Estadísticas preliminares*.

among higher income brackets.[19] In 2010, there were over 764,000 mobile broadband subscribers in Venezuela, making up approximately one third of the broadband market.[20]

Although there are 25 telecommunications operators in the country, CANTV, which was renationalized in 2007, monopolizes ADSL service and controls more than 90 percent of the internet market. There is some competition from cable modems, wireless broadband, and satellite connections. Inter places a distant second in the market and offers a triple package that includes cable television, cable modem, and telephone service.[21] CANTV has benefited financially from state ownership, particularly with regard to currency controls. For example, since January 2010, when the local currency was devalued, CANTV has been permitted to import a dollar for every 2.60 bolivares, while other firms in the sector have had to pay 4.30 bolivares per dollar.[22] CANTV's Movilnet also leads the mobile-phone market with 14 million subscribers,[23] out of a total of 29 million.[24] Two privately-owned companies also provide mobile-phone services: Digitel and Movistar. However, they have had to decrease their investments in infrastructure and have begun to ration their services because they are forced to use the higher private-sector exchange rate.[25] There are no special restrictions on the opening of cybercafes. CANTV's position as a dominant, state-owned ISP and mobile-phone provider has raised concerns about the ease with which systemic content filtering and surveillance could be implemented in the future. In recent years, there have been isolated incidents of CANTV engaging in censorship and monitoring when other providers have not (see below), but more systematic controls were not evident.

Advanced applications such as Facebook, Twitter, and the video-sharing site YouTube are freely accessible and growing in popularity.[26] On several occasions, however, international blog-hosting services have been temporarily blocked surrounding politically sensitive events. During the February 2009 constitutional referendum, bloggers and Twitter users reported that the site Blogger.com, which housed numerous Venezuelan blogs, was inaccessible to CANTV users for at least 24 hours.[27] Blocking allegations arose again during

[19] Hernan Galperin, *Tarifas y brecha de asequibilidad de los servicios de telefonía móvil en América Latina y el Caribe* [Rates and Breaches of Affordability of Mobile Telephone Services in Latin America and the Caribbean] (Lima: Diálogo Regional sobre Sociedad de la Información, 2010), available at http://dirsi.net/sites/default/files/DIRSI-ITIC-10-asequibilidad-movil-v1.1_3.pdf (in Spanish).

[20] Venezuela is one of five countries in the region with a mobile broadband penetration rate that is above the average rate of developed countries. ITU, *Perfiles Estadísticos*; Conatel, *Estadísticas preliminares*.

[21] BuddeComm, "Venezuela—Telecoms, Mobile, Broadband and Forecasts," http://www.budde.com.au/Research/Venezuela-Telecoms-Mobile-Broadband-and-Forecasts.html, accessed August 12, 2010.

[22] "Oswaldo Cisneros sigue apostándole a Venezuela: Digitel busca vías para consolidarse en 3G" [Oswaldo Cisneros Still Betting on Venezuela: Digitel Seeks Ways to Consolidate in 3G], Casetel, June 23, 2010, http://www.casetel.org/detalle_noticia.php?id_noticia=509 (in Spanish).

[23] "Los números oficiales de clientes de Cantv" [The Official Number of Clients of CANTV], *Inside Telecom* 11, no. 42, November 3, 2010, http://m.insidetele.com/newsletters.php?article_id=-3103130866257163706 (in Spanish).

[24] Conatel, *Estadísticas preliminares*.

[25] "Aún sin dólares para nuevas inversiones" [Even Without Dollars for New Investments], Casetel, August 23, 2010, http://www.casetel.org/detalle_noticia.php?id_noticia=637 (in Spanish).

[26] Alexa, "Top Sites in Venezuela," http://www.alexa.com/topsites/countries;0/VE, accessed December 20, 2010.

[27] See for example: http://www.cristalab.com/blog/chavez-y-cantv-bloquean-blogger-y-blogspot-ayer-en-venezuela-c68770l/.

the parliamentary elections on September 26, 2010. From September 24 to 27, blogs hosted by WordPress were inaccessible. Venezuelan bloggers claimed that CANTV blocked WordPress on the grounds that many of the sites it hosted were found to contain "illegally published" electoral content. However, an anonymous source at CANTV reportedly attributed the disruption to maintenance work on WordPress servers.[28] The government made no effort to clarify the situation.

The state acts as both the dominant service provider, through CANTV, and the sector's regulator and licensing authority, through Conatel. The president has the power to name and remove Conatel's director and the four members of its Directive Council. Although Article 35 of the Organic Law of Telecommunications provides for Conatel's operational and administrative autonomy, a series of presidential decrees over the past decade has shifted oversight of the commission to various ministries and finally to the vice president,[29] which has increased the agency's politicization.[30] Conatel has repeatedly demonstrated pro-government bias in decisions related to broadcast media, though it has not yet made comparable judgments affecting the internet or mobile-phone service.

LIMITS ON CONTENT

Although the Venezuelan authorities do not engage in systematic internet censorship, several measures have been taken to restrict the circulation of information deemed displeasing to the government, and officials have warned of their intention to control online content. According to free expression advocates, the objective of such measures is to gain the upper hand in a medium that is heavily used by the political opposition.

No systematic content blocking or cases of judicial censorship have been reported in Venezuela. However, since the renationalization of CANTV in 2007, there have been some incidents of blocks linked to sensitive political information. For example, days after the closure of the country's largest private television broadcaster, RCTV, in May 2007, two internet radio stations that transmit from Miami—Radionexx and CaracasRadioTV—began to be filtered by domain name. These are the first websites believed to have been censored by CANTV.[31] In April 2009, managers of *El Liberal Venezolano*, a blog of opposition-oriented

[28] David Sasaki, "Internet Censorship and Freedom of Expression in Latin America," Información Civica, November 1, 2010, http://informacioncivica.info/new/internet-censorship-and-freedom-of-expression-in-latin-america/.
[29] See Andrés Cañizález, "Conatel, la joya de la corona" [Conatel, the Jewel in the Crown], *Tal Cual*, August 9, 2010, http://www.talcualdigital.com/Blogs/Viewer.aspx?id=38920 (in Spanish).
[30] Jesús Urbina Serjant, "Venezuela," in *Las mordazas invisibles: Nuevas y viejas barreras a la diversidad en la radiodifusión* [Invisible Jaws: New and Old Barriers to Diversity in Broadcasting] (Montevideo: Program on Law and the Right to Communication, World Association of Community Radio [AMARC], 2009), http://legislaciones.amarc.org/mordazas/VEN_pais.htm (in Spanish).
[31] "Venezuela comienza el bloqueo de Internet" [Venezuela Starts Blocking the Internet], Noticias 24, May 31, 2007, http://www.noticias24.com/actualidad/noticia/5324/venezuela-comienza-el-bloqueo-de-internet/ (in Spanish).

political and economic opinion, reported blocking that affected CANTV clients.[32] In the period surrounding a controversial new monetary devaluation in January 2010, a well-known blog that published black-market exchange rates was blocked, along with some other sites providing similar information.[33] In May, it was reported that CANTV users could not access a website with content pertaining to violent crime and insecurity,[34] problems for which the government has drawn considerable public criticism.[35] These sites remained inaccessible to CANTV users through year's end, but those accessing the internet via Inter or mobile phones provided by Digitel reported being able to reach them. In the run-up to parliamentary elections in September 2010, the news-aggregator site Noticiero Digital, the 28th most popular website in the country,[36] was temporarily inaccessible from Venezuela via CANTV in addition to the above-mentioned blanket block on WordPress.[37] Separately, the sites of international human rights organizations like Freedom House, Reporters Without Borders, and Amnesty International are freely available.

The lack of clarity on whether the government is responsible for any of these cases of apparent blocking is compounded by the political situation in the country, in which there are no established checks and balances between the different branches of government, and the judiciary lacks independence. In this context, there is no transparent process or independent institutions through which website owners and content producers can pursue complaints of disruptions.

Although technical filtering has been limited, the authorities have taken steps to intimidate news portals and hosting companies, encouraging them to engage in self-censorship. This effort has centered recently on Noticiero Digital, known for its aggregation of content from other media outlets and the aggressively antigovernment viewpoints of its columnists and commenters. In 2007, it was already receiving approximately 450,000 daily

[32] "CANTV confirma bloqueo de El Liberal Venezolano" [CANTV Confirms Blocking of El Liberal Venezolano], *El Liberal Venezolano* (blog), April 15, 2009, http://liberal-venezolano.net/2009/04/15/cantv-confirma-bloqueo (in Spanish).

[33] Dollar.nu and Preciodolar.info. See "El Gobierno Venezolano Empezo a filtrar el Internet" [The Venezuelan Government Began to Filter the Internet], Ultraforos.com, January 6, 2010, http://www.ultraforos.com/foro/general/192628-el-gobierno-venezolano-empezo-filtrar-el-internet.html (in Spanish).

[34] Marianne Diaz, "Venezuela: Polémica por el bloqueo de páginas web por el ISP gubernamental" [Venezuela: Controversy Over Website Blocking by Government ISP], Global Voices, May 16, 2010, http://es.globalvoicesonline.org/2010/05/16/venezuela-polemica-por-el-bloqueo-de-paginas-web-por-el-isp-gubernamental/ (in Spanish).

[35] In August 2010, a special court for the protection of children and adolescents, responding to a request by the ombudsman's office, prohibited print media from publishing images of violence for a month. The measure was criticized as unconstitutional, and came shortly before legislative elections in September. Yolanda Valery, "Venezuela: cruce de racciones por prohibición de imágenes violentas" [Mixed Reactions to Prohibition of Violent Images], British Broadcasting Corporation (BBC), August 18, 2010, http://www.bbc.co.uk/mundo/america_latina/2010/08/100819_0145_venezuela_reacciones_prohiben_fotos_violentas_nacional_tal_cual_alf.shtml (in Spanish).

[36] Alexa, "Top Sites in Venezuela."

[37] David Sasaki, "Internet Censorship and Freedom of Expression in Latin America," Información Civica, November 1, 2010, http://informacioncivica.info/new/internet-censorship-and-freedom-of-expression-in-latin-america/; Noticiero Digital, "Carta abierta a CANTV, de parte de Noticiero Digital" [Open Letter to CANTV, from Noticiero Digital], news release, September 28, 2010, http://www.noticierodigital.com/forum/viewtopic.php?t=696877 (in Spanish).

visits. In March 2010, the attorney general began legal proceedings against the site for the publication in one of its forums of false information regarding the deaths of the minister of public works and housing and a well-known spokesman for the ruling party. The president demanded legal action because, in his words, "both one who says false information and one who allows it to be said and developed, are committing a crime."[38] In their reply, the editors of Noticiero Digital pointed out that although they do not arbitrarily censor their commentators, they have terms and conditions that participants agree to and which are rigorously enforced. They reported that the rumors were spread by two forum participants who had registered just minutes earlier and that once notified, site administrators acted rapidly to eliminate them and suspend the users.[39]

In March 2010, the attorney general asked the National Assembly to create legislation on the use of the internet by social media outlets. The legislature in turn issued a resolution instructing two of its committees to investigate websites that incite hatred and violence and lead to crime.[40] Reacting to the government pressure, some forums and pages specializing in news suspended their commentary systems, though the announced investigations have not yet led to any concrete legal restrictions or punishments. Some activists have suggested that the Noticiero Digital affair was orchestrated by the government with provocateurs posting the rumors in order to provide a pretext for intimidating websites and encouraging self-censorship.[41]

In June 2010, President Hugo Chávez alleged that an op-ed article published by Noticiero Digital was inciting a coup d'etat and demanded a criminal investigation. The site's managers argued that the author alone was responsible for what he wrote. The Public Ministry assigned two lawyers to open an investigation. Robert Carlo Olivares, author of the article in question, stopped collaborating with Noticiero Digital and refused to provide the site with information regarding his legal identification and address, as requested on behalf of the attorney general's office.[42] As with the earlier case, the results of the investigation remain unknown, but the site suspended registration of new forum participants as a preventative measure.

---

[38] "Noticiero Digital Responde a Acusaciones de Chávez" [Noticiero Digital Responds to Accusations by Chávez], *El Universal,* March 14, 2010, http://www.eluniversal.com/2010/03/14/pol_ava_noticiero-digital-re_14A3582451.shtml (in Spanish).

[39] Noticiero Digital, "Cómo dos foristas recien inscritos se aprovecharon de la libertad de ND y qué hicimos para controlarlos" [How Two Newly Registered Forum Members Took Advantage of the Freedom of ND and What We Did to Control Them], news release, March 16, 2010, http://www.noticierodigital.com/forum/viewtopic.php?t=631523 (in Spanish).

[40] *Gaceta Oficial* no. 39.389, March 18, 2010, http://www.tsj.gov.ve/gaceta/Marzo/1832010/1832010.pdf#page=1 (in Spanish).

[41] Marianne Diaz, "Venezuela: Algunas notas sobre el caso de Noticiero Digital" [Venezuela: Some Notes on the Noticiero Digital Case], Global Voices, April 19, 2010, http://es.globalvoicesonline.org/2010/04/19/venezuela-algunas-notas-sobre-el-caso-de-noticiero-digital/ (in Spanish).

[42] "ND le responde al ex columnista Roberto Carlo Olivares" [ND Responds to Former Columnist Roberto Carlo Olivares], Noticiero Digital, June 23, 2010, http://www.noticierodigital.com/2010/06/nd-le-responde-al-ex-columnista-roberto-carlo-olivares/ (in Spanish).

Although there are no specific regulations for conducting electoral campaigns using digital media, the National Electoral Council established some guidelines with Conatel ahead of the September 2010 parliamentary polls.[43] Twitter accounts of candidates, parties, and media outlets must comply with the general election rules, and candidates can only send three mass text messages per week per operator.

The Venezuelan authorities have taken measures to proactively influence online discussion, including via the pro-Chávez website www.aporrea.org. In January 2010, on a national television channel, Chávez encouraged members of his party to use Twitter to counteract the opposition. Shortly thereafter, in April 2010, Chavez opened his own Twitter account and by year's end had the largest number of followers in the country at approximately one million.[44] There are also some allegations that the government has attempted to influence online news coverage through the manipulation of advertising. Online media outlets critical of the government do not receive advertising revenue from state agencies and some private advertisers have been pressured to withdraw their funding from outlets like Noticiero Digital and Código Venezuela.

There are currently close to 130,000 Venezuelan websites, and social media have emerged as an important avenue for circulating information and expressing opinions at a time when independent television and radio stations have come under increased pressure. The country has the third-largest number of Facebook users in Latin America (about 7 million by the end of 2010)[45] and the largest number of Spanish-language Twitter users.[46] There are about 700,000 Venezuelan Twitter users, a figure that has grown by 1,000 percent in the last year, due in part to the president's recent instructions to his supporters to counteract his opponents on the platform.[47]

In addition to street demonstrations, which have been orchestrated through intensive use of SMS and BlackBerry Messenger,[48] activists have mounted notable campaigns on Twitter. The first of these, called #internetlujo, was launched in March 2009 to strengthen the effects of Decree 825, which declares access to the internet to be a political priority for

[43] "CNE se reunirá con Conatel el próximo martes para discutir la normativa de propaganda electoral" [Conatel and CNE will meet next Tuesday to discuss the rules of electoral propaganda], Venezolana de Televisión (VTV), August 22, 2010, http://www.vtv.gov.ve/noticias-nacionales/42430 (in Spanish).

[44] "Twitteros má populares en Venezuela" [Most Popular Twitters in Venezuela], Twitter-Venezuela, http://www.twitter-venezuela.com/ (in Spanish), accessed March 9, 2011.

[45] "Venezuela Facebook Statistics," Socialbakers, http://www.socialbakers.com/facebook-statistics/venezuela, accessed March 9, 2011.

[46] ComScore, "Indonesia, Brazil and Venezuela Lead Global Surge in Twitter Usage," press release, August 11, 2010, http://www.comscore.com/Press_Events/Press_Releases/2010/8/Indonesia_Brazil_and_Venezuela_Lead_Global_Surge_in_Twitter_Usage.

[47] "Venezuela, política 2.0," BBC, January 29, 2010, http://www.bbc.co.uk/mundo/america_latina/2010/01/100128_2205_venezuela_marchas_twitter_internet_jrg.shtml (in Spanish).

[48] Casto Ocando, "El Blackberry cambia batalla política en Venezuela" [Blackberry Changes Political Battle in Venezuela], *El Nuevo Herald*, September 10, 2009, http://www.elnuevoherald.com/2009/10/09/561909_p2/el-blackberry-cambia-batalla-politica.html (in Spanish).

the development of the country. The campaign was initiated primarily by professors and researchers from public universities to protest a subsequent presidential decree that characterized the public sector's use of the internet as a luxury and on those grounds restricted state investment in ICTs. An active community of bloggers, Twitter users, and others joined the campaign.[49] In July 2009, another Twitter-based campaign, #FreeMediaVe, was launched as a protest against the closure of 32 radio broadcasters by the government, and against a proposed Special Law Against Media Crimes, which was ultimately not submitted to the National Assembly for discussion.[50] Twitter also played a considerable role in campaigning for the September 2010 parliamentary elections, but like all online media, including news sites and online broadcasters, its use is strongest among the younger, wealthier, and more urban segments of the population.[51]

VIOLATIONS OF USER RIGHTS

While freedoms of speech and the press are constitutionally guaranteed, various laws have been used to restrict media and online freedom. Several individuals have been prosecuted in recent years for statements made via the internet or Twitter, though none were imprisoned as of the end of 2010. The courts are subject to the influence of the executive branch, particularly with regards to politically important cases, and the Supreme Court of Justice has passed down at least 10 judgments since 2001 that have placed curbs on freedom of expression.[52] The 2001 Special Law Against Information Crimes penalizes online activities involving privacy violations or pornography, but it has not been used to restrict online expression related to political or social matters.[53]

In December 2010, the National Assembly adopted a reform of the 2004 Law of Social Responsibility in Radio and Television (Resorte) that extended it to online and electronic media.[54] This lay the groundwork for censorship by websites and service providers of content transmitted by other users. Under the amended law, online media outlets are expected to establish mechanisms to restrict content that would violate the law,

[49] The campaign website is located at http://www.cecalc.ula.ve/internetprioritaria/, accessed August 18, 2010.
[50] Article 3 of the measure indicated that national independent producers, journalists, newscasters, lecturers, artists, and "any other person who expresses himself through any mode of communication" would be subject to criminal liability. See Pedro Pablo Peñaloza, "Todos los 'delitos mediáticos' se castigarán con cárcel" [All 'Media Crimes' Are Punishable by Imprisonment], *El Universal*, July 30, 2009, http://www.eluniversal.com/2009/07/30/pol_art_todos-los-delitos-m_1497998.shtml (in Spanish).
[51] Maria Isabel Neüman, "La participación en las redes sociales y las elecciones: ¿Los seguidores representan votos?" [Participation in Social Networks and the Elections: Do Followers Represent Votes?], *Experiencias Locales de Apropiación Technológica* (blog), October 21, 2010, http://apropiacion.blogspot.com/2010/10/la-participacion-en-las-redes-sociales.html#more (in Spanish).
[52] Juan Francisco Alonso, "'Jueces buscan limitar libre expresión'" ['Judges Seek to Limit Free Expression'], *El Universal*, August 21, 2010, http://politica.eluniversal.com/2010/08/21/pol_art_jueces-buscan-limit_2012844.shtml (in Spanish).
[53] The text of the law is available in Spanish at http://www.gobiernoenlinea.ve/docMgr/sharedfiles/LeyEspecialcontraDelitosInformaticos.pdf, accessed August 17, 2010.
[54] The amended law is available in Spanish at http://www.scribd.com/doc/45291089/Proyecto-de-Ley-de-Responsabilidad-en-Radio-Television-y-Medios-Electronicos, accessed December 19, 2010.

according to the Committee to Protect Journalists. Websites found in violation may be fined up to 13,000 bolivars ($US 3,000) and service providers who do not respond to government inquiries risk high fines and temporary suspension of operations.[55] Legislators also passed a law that deemed telecommunications networks and services to be of public rather than general interest, meaning they would be subject to greater state control.[56] These changes were among more than a dozen laws passed in the final days of the outgoing National Assembly, which was set to be replaced by a newly elected chamber with a substantial opposition minority.[57] The assembly also delegated its powers to the president for 18 months, allowing him to legislate by decree in areas including telecommunications and information technology.[58] When freedom of expression advocates demanded to participate in the lawmakers' deliberations,[59] they were harassed and assaulted by government supporters at the doors of the chamber.[60]

A 2005 reform of the penal code included significant restrictions on expression, especially in cases involving contempt or disrespect. Article 147 of the penal code stipulates that defamation of the president is punishable by 6 to 30 months in prison, while offenses against lower-ranking officials carry lighter punishments under Article 148.[61]

In addition, the penal code includes vague language criminalizing the dissemination of "false information." Article 297-A states: "Every individual who through false information spread by any print media, radio, television, telephone, e-mail, or written pamphlet causes

[55] "CPJ Condemns Two Media Laws," International Freedom of Expression eXchange (IFEX), December 22, 2010, http://www.ifex.org/venezuela/2010/12/22/two_reforms_approved/.

[56] The amended law is available in Spanish at http://www.scribd.com/doc/45293016/Nueva-Ley-Organica-de-Telecomunicaciones, accessed December 19, 2010.

[57] Sara Carolina Díaz, "En 15 días Asamblea aprobó 16 leyes" [In 15 Days Assembly Approves 16 Laws], *El Universal*, December 19, 2010, http://politica.eluniversal.com/2010/12/19/pol_art_en-15-dias-asamblea_2141341.shtml (in Spanish).

[58] "Texto de la Ley Habilitante entregada al la AN" [Text of the Enabling Act Submitted to the National Assembly], Panorama.com.ve, December 14, 2010, http://www.panorama.com.ve/14-12-2010/avances/0chavez-martes-emergencia2.html (in Spanish).

[59] "Periodistas y ONG solicitan audiencia a la AN para defender la libertad de expresión" [Journalists and NGOs Seek Hearing at the National Assembly to Defend Freedom of Expression], *El Nacional*, December 16, 2010, http://www.el-nacional.com/www/site/p_contenido.php?q=nodo/172357/Naci%C3%B3n/Periodistas-y-ONG-solicitan-audiencia-a-la-AN-para-defender-la-libertad-de-expresi%C3%B3n (in Spanish); "Esperamos respuesta oportuna de AN a documento Por una internet de contenido libre" [We Expect a Timely Response from the National Assembly to Document 'For an Internet of Free Content'], *Todos en Red* (blog), December 17, 2010, http://todosenred.wordpress.com/2010/12/17/esperamos-respuesta-oportuna-de-an-a-documento-por-una-internet-de-contenido-libre/ (in Spanish).

[60] Patty Fuentes Gimón, "Respuesta oficial" [Official Response], *Tal Cual*, December 17, 2010, http://www.talcualdigital.com/Avances/Viewer.aspx?id=45795&secid=28 (in Spanish).

[61] Every opinion or manifestation of dissent made in public or in private against a government employee can be considered an offense. The new penal code has been described as an attempt to criminalize political opposition. For more information, see Súmate, "Respeto a la libertad de expresión: ¿Limita el código penal la libertad de expresión?" [Respect for Freedom of Expression: Does the Penal Code Limit Freedom of Expression?], http://infovenezuela.org/democracy/cap4_es_2.htm (in Spanish), accessed August 22, 2010.

[61] Every opinion or manifestation of dissent made in public or in private against a government employee can be considered an offense. The new penal code has been described as an attempt to criminalize political opposition. For more information, see Súmate, "Respeto a la libertad de expresión: ¿Limita el código penal la libertad de expresión?" [Respect for Freedom of Expression: Does the Penal Code Limit Freedom of Expression?], http://infovenezuela.org/democracy/cap4_es_2.htm (in Spanish), accessed August 22, 2010.

collective panic or anxiety, will be punished with two to five years in prison."[62] Given that the internet is classified as a channel of mass distribution of information, some violations of the penal code (such as defamation or incitement of hatred or rebellion) may be considered more severe online than in other media forms.[63]

Over the past two years, at least five people have been charged or arbitrarily detained for online expression on politically relevant topics. In July 2010, police detained two people for alleged involvement in the spread via Twitter of false rumors aimed at destabilizing the national banking system. The incident came in the wake of the closure or nationalization of more than 10 banks during 2009. The suspects were charged with spreading false information under the General Law on Banks and Other Financial Institutions, reformed in 2009, which calls for prison sentences of 9 to 11 years. Strangely, one suspect, Luis Acosta Oxford, had barely 32 Twitter followers and had sent 201 messages at the time of his detention, and only one of the messages had referred to the banking situation.[64] The other suspect, Carmen Cecilia Nares Castro, had been subscribed to Twitter for just two months and had only six followers. The authorities ultimately determined that the arrests had been a mistake, and Nares's lawyer criticized the attorney general's office for failing to conduct adequate investigations.[65]

Two months later, police arrested a 27-year-old employee of the state electric company, Jesus Majano, for allegedly sharing via Twitter offensive words and images that encouraged the assassination of President Chávez. After several hours of detention under Article 285 of the penal code, he was provisionally released pending additonal hearings.[66] In November, Cristian Fuentes, a social communications student and regular user of the account @Caracasmetro, a tool created to monitor the subway system's operation, was arrested while taking photographs in the subway. He reported that the police told him he

[62] *Gaceta Oficial* no. 5.763 Extraordinario, March 16, 2005, http://www.tsj.gov.ve/gaceta_ext/marzo/160305/160305-5763-01.html (in Spanish).

[63] Rafael Martínez, "Twitter: Esos Malditos 140 Caracteres" [Twitter: Those Damned 140 Characters], SoyRafael.com, February 22, 1010, http://soyrafael.com/2010/02/22/twitter-esos-malditos-140-caracteres/ (in Spanish). Article 285 of the penal code states: "Anyone who incites disobedience of the laws or hatred among its people or makes apology for acts that the law provides as crimes, so as to endanger the public peace, shall be punished with imprisonment of three years to six years."

[64] "El tweet 'desestabilizador'" [The 'Destabilizing' Tweet], Código Venezuela, July 8, 2010, http://www.codigovenezuela.com/2010/07/el-tweet-desestabilizador/ (in Spanish).

[65] National Assembly, "Imputada en caso de desestabilización bancaria niega su responsabilidad" [Suspect in Case of Bank Destabilization Denies Responsibility], news release, July 21, 2010, http://www.asambleanacional.gob.ve/index.php?option=com_content&view=article&id=26011:imputada-en-caso-de-desestabilizacion-bancaria-niega-su-responsabilidad-&Itemid=50&lang=es (in Spanish); Reporters Without Borders, "Twitter Users Formally Charged, Banned from Posting Messages," IFEX, July 14, 2010, http://www.ifex.org/venezuela/2010/07/14/twitter_users_arrested/.

[66] "Designan a Fiscal en caso de twittero por incitar al magnicidio" [Prosecutor Assigned in Case of Twitterer Charged with Inciting Assassination], *La Patilla*, September 9, 2010, http://www.lapatilla.com/site/2010/09/09/cicpc-detuvo-a-trabajador-de-corpoelec-por-incitar-al-magnicidio-a-traves-de-twitter/ (in Spanish); "Venezuelan Released After Arrest for Twitter Post," Associated Press, September 10, 2010, http://www.boston.com/news/world/latinamerica/articles/2010/09/10/venezuelan_released_after_arrest_for_twitter_post/.

was being detained because they were sure he would post the photos on Twitter.[67] After a few hours Fuentes was released without charges.

In another case, in March 2006, a judge ordered the pretrial detention of Gustavo Azócar, a newscaster and political commentator for the local television station Televisora del Tachira, and a correspondent for the national daily *El Universal*. Azócar was facing trial on charges of illegal profit, fraud, and forgery, but the case appeared to be a politically motivated retaliation for his regular criticism of the government. Fifteen days after the detention order, Azócar won the right to be judged while remaining outside custody, on the condition, among some others, that he refrain from speaking publicly about the case. In July 2009 he was returned to prison for publishing on his website articles that his colleagues had written about his case. In March 2010 he was convicted of the original crimes and sentenced to two years and six months in prison. Since he had already served eight months behind bars and his supposed crimes were not serious, he was allowed to remain free, though he must report regularly to the courts.[68]

The constitution prohibits anonymity,[69] and the rule applies to all media. Since 2005,[70] Conatel has required mobile-phone operators to collect copies of their subscribers' identity documents, address, fingerprints, and signature. According to the Computer Crimes Act, this information must be delivered to the state security agencies upon request. The service providers are also obliged to keep detailed logs of all calls, including the phone number of the caller, the destination phone number, the date, time, and duration of the call, the location and direction of the base station where the call is initiated, and the location and direction of the base station where the call is received, provided it belongs to the same network. The Law Against Kidnapping and Extortion obliges the providers of telecommunications, banking, or financial services to supply required data to the Public Ministry upon request. National Assembly deputies from the ruling party have reported receiving complaints from law enforcement agencies that only the state-owned Movilnet provides information immediately.[71] Cybercafe customers are not required to register their identity documents to gain internet access, and there are no known cases in which such users' activities have been tracked.

---

[67] "'Seguiré usando el Metro y denunciando fallas del servicio'" [Will Continue Using the Metro and Reporting Service Failures], *El Universal*, November 3, 2010, http://www.eluniversal.com/2010/11/03/ccs_art_seguire-usando-el-m_2090854.shtml (in Spanish); IPYS, "Journalist Briefly Detained by Police," IFEX, November 4, 2010, http://www.ifex.org/venezuela/2010/11/04/fuentes_detained/.

[68]; Daniel Cancel, "Gustavo Azócar Released on Parole," *Latin America Herald Tribune,* http://laht.com/article.asp?CategoryId=10717&ArticleId=231941; http://cpj.org/2010/03/venezuela-journalist-azocar-convicted-on-retaliato.php, accessed March 9, 2011.

[69] Article 57: "Everyone has the right to freely express their thoughts, ideas or opinions orally, in writing or any other form of expression, and to make use of any means of communication and diffusion, and no censorship shall be established. Anyone making use of this right assumes full responsibility for everything expressed. Anonymity, war propaganda, discriminatory messages or those promoting religious intolerance are not allowed."

[70] *Gaceta Oficial* no. 38.157, April 1, 2005, http://www.tsj.gov.ve/gaceta/abril/010405/010405-38157-20.html (in Spanish).

[71] "Presionan a brindar información personal" [Pressure to Provide Personal Information], BlackBerryVzla.com, June 24, 2010, http://www.blackberryvzla.com/2010/06/presionan-brindar-informacion-personal.html (in Spanish).

Article 22 of the Special Law Against Information Crimes penalizes disclosure, dissemination, or misuse of personal information with two to six years in prison and heavy fines. Nevertheless, opinion programs transmitted by the state-owned television channel regularly air recordings of government opponents' telephone conversations, and no investigations or sanctions have ever resulted from the disclosures.

In July 2007, journalist Roger Santodomingo resigned as director of Noticiero Digital after his son received threats and his car was set on fire in front of his house.[72] However, this has been the only case of its kind to date. There have been no reported instances of hacking or denial-of-service attacks on opposition websites.

[72] "'Estalló camioneta del periodista Roger Santodomingo" [Journalist Roger Santodomingo's Truck 'Exploded'], Correo del Caroní, July 5, 2007, http://www.correodelcaroni.com/archivo/archivo.php?id=71460 (in Spanish).

VIETNAM

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Not Free**
Obstacles to Access	n/a	16
Limits on Content	n/a	25
Violations of User Rights	n/a	32
Total	**n/a**	**73**

POPULATION: 88.9 million
INTERNET PENETRATION: 31 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
SUBSTANTIAL POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

The internet in Vietnam has undergone impressive development over the past decade, and is now accessed by over a quarter of the population. Since the medium's introduction in 1997, the ruling Vietnamese Communist Party (VCP) has demonstrated concern that the internet could be used to challenge its monopoly on political power, leading to contradictory policies designed to support or suppress online activities.

In recent years, the government has invested in expanding citizens' access to information and communication technologies (ICTs), as seen in the so-called Taking-Off Strategy 2011–2020,[1] which aims to raise Vietnam's ICT sector to the level of its regional neighbors. At the same time, the government has intensified its efforts to monitor and censor online content. After a relative easing of repression from 2004 to 2006 as Vietnam prepared to host an Asia-Pacific Economic Cooperation summit and join the World Trade Organization, the environment for free expression has deteriorated, and a growing number of bloggers have faced arrest, harassment, and imprisonment. In 2009, the New York–based Committee to Protect Journalists (CPJ) listed Vietnam among the 10 most repressive countries for bloggers.[2] In late 2009 and throughout 2010, a series of cyberattacks targeting a wide range of websites that were critical of the government highlighted an additional threat to internet freedom both within and beyond Vietnam's borders. The environment

[1] Business in Asia, "Taking-off Strategy," http://www.business-in-asia.com/vietnam/vietnam_ict.html, accessed August 25, 2010.
[2] Committee to Protect Journalists, "10 Worst Countries to Be a Blogger," April 30, 2009, http://www.cpj.org/reports/2009/04/10-worst-countries-to-be-a-blogger.php.

tightened further towards year's end, as the authorities prepared for a Communist Party Congress in January 2011.

OBSTACLES TO ACCESS

Thanks to decreasing costs and the improvement of electricity and telecommunications networks, Vietnam's internet penetration rate has grown dramatically over the past decade, from 0.3 percent in 2000 to nearly 30 percent (25 million users) in 2010.[3] ADSL broadband access is also widely available and estimated to have five million users as of 2010. The internet's growth is largely driven by the demands of Vietnam's relatively young population; some 60 percent of the country's total population is under 35. Internet access points are easily found in urban areas throughout the country. In most towns, citizens can access the internet in their homes and workplaces. Cybercafes are affordable for most urban dwellers,[4] and WiFi connections are available free of charge in many semi-public spaces such as airports, cafes, restaurants, and hotels. Given Vietnam's 92 percent literacy rate, illiteracy does not pose a barrier to access.[5] The availability of the internet in rural areas remains limited, although programs backed by the government and international donors have increased access in recent years. Ethnic minorities and the poor live primarily in remote areas and are especially at a disadvantage.

Vietnam was home to 88.5 million mobile-phone users in 2009, according to the ITU.[6] The country's Ministry of Information and Communications (MIC) placed the number at 110 million in early 2010. Although the figures exceed the total population, it is estimated that some 30 million low-income Vietnamese lack mobile phones, while others own two mobile devices or multiple SIM cards.[7] A third-generation technology (3G) network enabling internet access via mobile phones has been operating since the end of 2009, and the number of users is slowly expanding. As of mid-2010, there were at least 7 million 3G users.[8]

[3] Vietnam Internet Network Information Center, "Report on Internet Statistics of Vietnam," September 2010, http://www.thongkeinternet.vn/jsp/thegioi/dna_tab.jsp. International Telecommunication Union (ITU) shows the penetration rate at approximately 27 percent (23 million users) as of 2009. For more information see "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx.

[4] "Vietnam: 20% Do Not Trust Internet Information," P.A News, April 15, 2010, http://news.pavietnam.vn/archives/1547 (in Vietnamese).

[5] UNICEF, "At a Glance: Vietnam," http://www.unicef.org/infobycountry/vietnam_statistics.html, accessed August 25, 2010.

[6] International Telecommunication Union, "ICT Statistics 2009—Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx, accessed August 25, 2010.

[7] "Mobile Subscribers Touch 110 Million in 2009," Viet Nam Business News, March 7, 2010, http://vietnambusiness.asia/mobile-subscribers-touch-110-million-in-2009/.

[8] Ha Phuong, "Mobile Operators Magnify Numbers of 3G Subscribers," Look at Vietnam, June 12, 2010, http://www.lookatvietnam.com/2010/06/mobile-operators-magnify-numbers-of-3g-subscribers.html.

The video-sharing website YouTube, the microblogging application Twitter, and international blog-hosting services are freely available and growing in popularity. However, in September 2009 an order in which the Ministry of Public Security (MPS) instructed internet-service providers (ISPs) to block Facebook, which had roughly a million users in Vietnam at the time,[9] began circulating online.[10] By November, users were reporting difficulty accessing the website. It remained sporadically inaccessible throughout 2010, but the government refused to officially acknowledge trying to block.[11] While no laws prohibit the use of circumvention tools, a 2008 decree makes it illegal to access blocked websites.[12] Nevertheless, information on circumventing the block on Facebook circulated fairly widely, including via videos and blog posts.[13] As such, by the end of 2010, the number of Facebook users in Vietnam had increased to nearly 2 million despite the block,[14] though some users complained that previous, relatively simple methods of circumvention were becoming less effective. Zing Me, a domestic social networking site, had five million users by early 2011.[15] In May 2010, the Ministry of Information and Culture (MIC) also launched a government-backed social network called Go VN, where users must register with their real name and government-issued identity number when creating an account; the initial response to the new initiative was limited.[16]

The three biggest ISPs are the state-owned Vietnam Post and Telecommunications (VNPT), which holds 74 percent of the market, the military-owned Viettel (11 percent), and the privately owned FPT (10 percent). VNPT and Viettel also own the three largest mobile-phone service providers in the country (MobiFone, VinaPhone, and Viettel), which reportedly serve 100 million of Vietnam's 110 million users. Four privately owned companies share the remainder.[17] While there is no legally imposed monopoly for access providers, informal practices create hurdles for new companies seeking to enter the market,

[9] An Khanh, "Online Business to Attract Young," Radio Free Asia, July 21, 2010, http://www.rfamobile.org/vietnamese/in_depth/vietnamese-youth-is-attractted-to-do-business-on-facebook-KAn-07212010160732.html (in Vietnamese).

[10] Viet Tan, "Decree to Block Facebook in Vietnam," September 1, 2010, http://www.viettan.org/spip.php?article9390; "Vietnam Is No Longer Friends with Facebook," Deutsche Presse-Agentur, December 21, 2009, available at http://www.viettan.org/spip.php?article9335.

[11] "Vietnam to Block Facebook," CNN iReport, November 10, 2009, http://ireport.cnn.com/docs/DOC-354181.

[12] Ministry of Information and Communications, Decree 97/2008/NĐ-CP, "Regarding the management, provision and use of Internet services and electronic information on the internet," issued August 28, 2008, http://mic.gov.vn/VBQPPL/vn/documentdetail/8769/index.mic.

[13] Brannon Cullum, "Spotlighting Digital Activism in Vietnam," Movements.org, November 2, 2010, http://www.movements.org/blog/entry/spolighting-digital-activism-in-vietnam/.

[14] "Vietnam Facebook Statistics," Socialbakers, http://www.socialbakers.com/facebook-statistics/vietnam, accessed February 24, 2011.

[15] Huyen Chip. "Vietnam: State of Social Media One Year After Facebook Block", Global Voices, January 25, 2011, http://globalvoicesonline.org/2011/01/25/vietnam-state-of-social-media-one-year-after-facebook-block/.

[16] James Hookway, "In Vietnam, State 'Friends' You," *Wall Street Journal*, October 4, 2010, http://online.wsj.com/article/SB10001424052748703305004575503561540612900.html.

[17] "2010: What Will the Mobile Communication Market Be Like?" Hanoimoi Online, March 5, 2010, http://www.hanoimoi.com.vn/newsdetail/Kinh_te/312116/nam-2010-thi-truong-thong-tin-di-dong-se-ra-sao.htm (in Vietnamese); "Mobile Subscribers Touch 110 Million in 2009," Viet Nam Business News.

and many find that they lack the political ties or economic clout to do so. Similarly, there is a concentration of internet-exchange providers (IXPs), which serve as gateways to the international internet. Currently there are seven IXPs, five of which are state- or military-owned.[18]

The Ministry of Post and Telecommunications (MPT), the MPS, and the Ministry of Culture, Sport, and Tourism (MCST) regulate the management, provision, and usage of internet services. On paper, the MCST is charged with regulating sexual or violent content, while the MPS oversees measures related to politically sensitive content. In practice, however, the ruling VCP issues guidelines to all regulatory bodies as it deems appropriate and in a largely nontransparent manner. The Vietnam Internet Network Information Center (VNNIC), run by the MPT, manages and allocates internet resources such as domain names.[19]

LIMITS ON CONTENT

While the Vietnamese government has fewer resources to devote to online content control than its counterpart in China, the authorities have nonetheless established an effective and increasingly sophisticated content-filtering system. Censorship of online content is implemented by ISPs rather than at the backbone level or the international gateway. There is no real-time filtering based on keywords or using deep-packet inspection. Instead, specific URLs are identified in advance as targets for censorship and placed on blacklists; ISPs are legally required to block these URLs. In some instances, when users attempt to access a censored website, a "blocked page" notification will appear, informing them that the page has been deliberately blocked rather than rendered unavailable by a technical failure. However, users sometimes receive a vague error message indicating simply that the browser was unable to locate the server for that website.

Although the censorship system is ostensibly aimed at limiting access to sexually explicit content, in practice it primarily targets sites deemed threatening to the VCP's monopoly on political power, such as those related to Vietnamese political dissidents, human rights, and democracy. Websites on religious freedom, Buddhism, Roman Catholicism, and the Cao Dai religious group are blocked to a lesser but still significant degree.[20] The Vietnamese authorities largely focus their censorship efforts on Vietnamese-language content, blocking English-language sites less often. For example, while the

[18] The five are VNPT, Viettel, EVN Telecom, Hanoi Telecom, and VTC.
[19] Vietnam Internet Network Information Center, "Regulation on Registrar of Domain Name Dot Vn," March 5, 2007, http://www.vnnic.vn/english/5-6-300-0-2-01-20071115.htm.
[20] "Vietnamese Government Expands Internet Censorship to Block Catholic Websites," Catholic News Agency, August 6, 2009, http://www.catholicnewsagency.com/news/vietnamese_government_expands_internet_censorship_to_block_catholic_websites/.

websites of the *New York Times*, the British Broadcasting Corporation, Freedom House, Amnesty International, and Human Rights Watch are accessible, those of overseas Vietnamese organizations that are critical of the government—such as talawas.org, danluan.org, or danchimviet.com—are blocked. The websites of the Vietnamese-language services of the U.S.-funded Radio Free Asia and Voice of America outlets are also sporadically blocked.

In recent years, the online filtering apparatus has expanded. Both the social-networking website Facebook and content related to border disputes between China and Vietnam, for example, were freely available several years ago but were restricted as of the end of 2010. Because of the unpredictable and nontransparent way in which topics become forbidden, it is difficult for users to know where exactly the "red lines" lie. As a result, many media workers and online writers practice self-censorship or publish under pseudonyms. One common form of self-censorship is for bloggers to disable the readers' comment option on their writings. This acts as a precautionary measure to prevent discussion by commentators from taking a more confrontational tone than what was intended by the original posting.

Online media outlets and internet portals are state owned and therefore subject to censorship by the VCP. The party's Department for Culture and Ideology and the MPS regularly instruct online newspapers or portals to remove content they perceive as critical of the government. Editors and journalists who post such content risk disciplinary warnings, job loss, or even imprisonment. In October 2008, the MIC announced the creation of the Administrative Agency for Radio, Television, and Electronic Information. Among other duties, the agency was tasked with regulating online content, including by drafting guidelines for blogs, though the full extent of its activities remained unclear as of the end of 2010.[21] In December 2008, the MIC announced a directive requiring blogging platforms to remove "harmful" content, report to the government every six months, and provide information about individual bloggers upon request.[22] This has generally resulted in an increase in the censorship of content that is critical of the VCP, but the impact has been less significant on the many blogs hosted outside the country. In late 2008, the deputy minister of information and communications reportedly said he would contact international companies such as Google and Yahoo! to request cooperation on censorship. However, as of 2010 there were no indications that these companies were assisting the Vietnamese authorities, for instance by self-censoring search results, as is done in China.[23]

[21] Geoffrey Cain, "Bloggers the New Rebels in Vietnam," SFGate.com, December 14, 2008, http://articles.sfgate.com/2008-12-14/news/17131885_1_bloggers-communist-party-vietnam; Xuan Linh, "Watchdog to Regulate Blogs in Vietnam," VietnamNet Bridge, October 3, 2008, http://english.vietnamnet.vn/politics/2008/10/806781/.

[22] Karin Deutsch Karlekar, ed., "Vietnam," in *Freedom of the Press 2009* (New York: Freedom House, 2009), http://www.freedomhouse.org/template.cfm?page=251&year=2009.

[23] Ann Binlot, "Vietnam's Bloggers Face Government Crackdown," *Time*, December 30, 2008, http://www.time.com/time/world/article/0,8599,1869130,00.html.

There is no avenue for managers of blocked websites to appeal censorship decisions. There have been no reports of restrictions placed on content transmitted via e-mail or mobile-phone text messages.

Despite the government restrictions, Vietnam's internet is vibrant and offers a diversity of content in the Vietnamese language, though most of it is nonpolitical. According to the MIC, there were 1.1 million blogs in Vietnam as of October 2008.[24] In recent years, Yahoo! 360 emerged as an extremely popular platform for the blogging community, and for individual bloggers writing on entertainment, fashion, or politics to gain a large number of followers. At the height of its popularity, the application reportedly had 15 million Vietnamese users, including 2 million who updated their pages daily.[25] However, as the program was not particularly popular outside Vietnam, in mid-2009 Yahoo! terminated the service. Since then, Vietnam's blogging community has become much more dispersed, with some bloggers migrating to Blogger.com or WordPress.com, others to Yahoo!'s 360Plus, and especially to Facebook and Multiply. Between May 2009 and November 2009, shortly before the government restricted access to Facebook, the number of Facebook users from Vietnam reportedly increased from 72,000 to one million.[26]

Although most blogs address personal or nonpolitical topics, citizen journalism has emerged as an important phenomenon and a source of information for many Vietnamese, particularly given the VCP's tight control over traditional media. Websites such as Vietnam Net and Vietnam News discuss subjects like corruption, social justice, and the country's political situation. According to one study, citizen journalists in recent years have exposed stories such as blunders by the Ministry of Construction surrounding a bridge collapse, corruption in transportation projects funded by Japanese foreign aid, and police brutality against farmers protesting against land grabs.[27] Blogs and online writings have also played a critical role in mobilizing public opinion and even "real life" protests over environmental concerns related to mining projects in the Central Highlands, and disputes with China over the Paracel and Spratly Islands. In early 2009, a petition was circulated calling on the authorities to reconsider plans to mine the mineral bauxite in cooperation with a Chinese state-owned company. The petition garnered thousands of signatures. The campaign organizers then launched a website called Bauxite Vietnam that attracted millions of hits, although it is hosted on a server in France.[28] Some bloggers and activists also used the internet to distribute t-shirts criticizing the bauxite policy and China's claims to the disputed

[24] Linh, "Watchdog to Regulate Blogs in Vietnam."
[25] Aryeh Sternberg, "Vietnam Online: Then and Now," iMedia Connection, January 5, 2010, http://www.imediaconnection.com/content/25480.asp.
[26] Ibid.
[27] Viet Tan, "Vietnam's Blogger Movement: A Virtual Civil Society in the Midst of Government Repression," March 30, 2009, http://www.viettan.org/spip.php?article8421.
[28] Viet Tan, "Denial of Service: Cyberattacks by the Vietnamese Government," April 27, 2010, http://www.viettan.org/spip.php?article9749. The Bauxite Vietnam website is located at http://www.bauxitevietnam.info.

islands.[29] Methods to circumvent censorship, such as the use of proxy servers, are relatively well-known among the young and technology-savvy internet users in Vietnam, with some searchable via Google.

VIOLATIONS OF USER RIGHTS

The constitution affirms the right to freedom of expression, but media are strictly controlled by the VCP in practice. Legislation including internet-related decrees, the penal code, the Publishing Law, and the State Secrets Protection Ordinance restrict free expression, and have been used to imprison journalists and bloggers. The judiciary is not independent, and many trials related to free expression last only a few hours. When detaining bloggers and online activists, police routinely fail to follow Vietnamese legal provisions, arresting individuals without a warrant, or retaining them in custody beyond the maximum period allowed by law. In an effort to expand traditional media controls to the blogosphere, the MIC issued Circular 7 in December 2008. It requires blogs to address only strictly personal information, and refrain from political or social commentary. It also bars internet users from disseminating press articles, literary works, or other publications that are prohibited by the Press Law.[30]

In recent years, the Vietnamese authorities have embarked on several crackdowns against bloggers and online writers, subjecting them to extended interrogations, imprisonment, and in some instances physical abuse.[31] In one of the first cases of a prominent blogger being imprisoned, Dieu Cay, a vocal critic of the government's human rights record and an advocate for Vietnamese sovereignty over the Spratly Islands, was sentenced in late 2008 to 2.5 years in prison on tax evasion charges that most observers viewed as politically motivated.[32] Other bloggers have been prosecuted and convicted for "subversion" or "attempting to overthrow the people's government." The authorities have also invoked Articles 79 and 88 of the penal code to imprison bloggers and online activists.[33] In January 2010, a court in Ho Chi Minh City sentenced four prodemocracy activists to a total of 33 years in prison for using the internet to report rights violations or disseminate pro-democracy views. Of the four, Le Cong Dinh and Le Thang Long each received 5 years,

[29] John Ruwitch, "Vietnam Bloggers Arrested Over China Shirt Protest," Reuters, September 5, 2009, http://www.reuters.com/article/idUSTRE5840CY20090905.
[30] Reporters Without Borders, "Internet Enemies: Vietnam," http://en.rsf.org/internet-enemie-viet-nam,36694.html, accessed August 25, 2010.
[31] "Vietnam's Internet Crackdown," CNN Video, June 18, 2010, http://edition.cnn.com/video/#/video/world/2010/06/18/stevens.vietnam.internet.crackdown.cnn?iref=allsearch.
[32] Human Rights Watch, "Banned, Censored, Harassed and Jailed," news release, October 11, 2009, http://www.hrw.org/en/news/2009/10/11/banned-censored-harassed-and-jailed.
[33] Reporters Without Borders, "Internet Enemies: Vietnam."

Nguyen Tien Trung received 7 years, and Tran Huynh Duy Thuc received 16 years.[34] In late 2009, three other individuals were sentenced to prison for views expressed on the internet: Pham Van Troi, a poet sentenced to four years; Vu Van Hung, a former teacher sentenced to three years; and Tran Duc Thach, a poet sentenced to three years.[35] As of July 2010, Global Voices Online had compiled a list of 10 jailed online activists in Vietnam.[36]

In addition to imprisonment, bloggers and online activists have been subjected to physical attacks, job loss, termination of personal internet services, and travel restrictions. In May 2010, Lu Thi Thu Trang, an online activist associated with the pro-democracy movement Bloc 8406, was beaten by police in front of her five-year-old son, and then detained for interrogation.[37] In June 2009, popular blogger Huy Duc was fired from his job with a state-owned newspaper after it came under government pressure over postings he had written condemning the Berlin Wall.[38] In May 2010, provincial authorities terminated the telephone and internet-service connection at the home of Ha Si Phu, one of Vietnam's best-known dissident bloggers, alleging that he had used his telephone line to transmit "antigovernment" information. Also in May 2010, police detained and interrogated two bloggers, Uyen Vu and Trang Dem, at Tan Son Nhat airport in Ho Chi Minh City, and barred them from traveling abroad for their honeymoon.[39] In Oct 2010, blogger Le Nguyen Huong Tra (who uses the penname Do Long Girl) was detained on charges of "misusing democratic rights to violate the state's and citizens' interests," after she reported about the family affairs of a high-ranking official.[40] That same month, blogger Phan Thanh Hai (who uses the penname Anh Ba Sai Gon) was arrested on charges of distributing false information on his blog.[41] The incidents occurred as part of a broader crackdown on free expression in the lead up to an important Communist Party Congress in January 2011.

The Vietnamese authorities employ both technology-based and "low-tech" methods for monitoring online communications. The former include monitoring web traffic and e-mails, especially of political activists, while the latter involve shadowing the movements of known online activists. Cybercafe owners are required to install special software to track

[34] Reporters Without Borders, "Court Sentences Four Netizens and Pro-Democracy Activists to a Total of 33 Years in Jail," news release, January 20, 2010, http://en.rsf.org/vietnam-court-sentences-four-netizens-and-20-01-2010,36156.html.
[35] Human Rights Watch, "Banned, Censored, Harassed, and Jailed," August 4, 2010, http://www.hrw.org/en/news/2010/08/04/banned-censored-harassed-and-jailed.
[36] Threatened Voices, "Bloggers: Vietnam," Global Voices Advocacy, http://threatened.globalvoicesonline.org/bloggers/vietnam, accessed August 26, 2010.
[37] "Government Suppression of Bloggers and Websites," VietCatholic News, May 27, 2010, http://www.vietcatholic.org/News/Clients/ReadArticle.aspx?ID=80607 (in Vietnamese).
[38] Viet Tan, "Denial of Service: Cyberattacks by the Vietnamese Government."
[39] Human Rights Watch, "Vietnam: Stop Cyber Attacks Against Online Critics," news release, May 26, 2010, http://www.hrw.org/en/news/2010/05/26/vietnam-stop-cyber-attacks-against-online-critics.
[40] Vu Mai and Quoc Thang, "Blogger Co Gai Do Long Urgently Arrested," VN Express, October 26, 2010, http://vnexpress.net/GL/Phap-luat/2010/10/3BA221C2/ (in Vietnamese).
[41] "Another blogger arrested in Vietnam crackdown", Committee to Protect Journalists (CPJ), October 28, 2010, http://cpj.org/2010/10/another-blogger-arrested-in-vietnam-crackdown.php.

and store information about their clients' online activities.[42] In addition, citizens are obliged to provide the details of their government-issued identification documents to register with their ISP when purchasing a home internet connection. In late 2009, the MIC announced that all prepaid mobile-phone subscribers would be required to register their details with the operator. Individuals are allowed to register only up to three numbers per carrier.[43] The government argues that such measures are necessary to counter mass text-message advertising that plagues many Vietnamese phone users. However, the steps also facilitate surveillance, as service providers are required to share information about users with the government upon request. Nevertheless, there are no requirements for real-name registration when blogging or posting online comments, and many Vietnamese do so anonymously.

The intensified harassment of bloggers in 2009 and 2010 has coincided with systematic cyberattacks targeting individual blogs as well as websites run by other activists in Vietnam and abroad.[44] Since September 2009, dozens of sites have been attacked, including those operated by Catholics who criticize government confiscation of Church property, forums featuring political discussions, and the website raising environmental concerns surrounding bauxite mining.[45] The attackers infected computers with malicious software disguised as a popular keyboard program that allows Microsoft Windows to support the Vietnamese language. Once infected, computers became part of a "botnet" whose command-and-control servers were primarily accessed from internet protocol (IP) addresses inside Vietnam. The network of hijacked computers was then used to carry out the denial-of-service attacks described above. Both McAfee, a major internet security firm, and Google reported on the sophisticated attacks, with the latter estimating that "potentially tens of thousands of computers" had been affected, most of which belonged to Vietnamese speakers.[46] McAfee stated that "the perpetrators may have political motivations, and may have some allegiance to the government of the Socialist Republic of Vietnam."[47] The Vietnamese authorities have not taken measures to find or punish the attackers. On the contrary, during a national conference on media held in May 2010, the MPS announced that it had "destroyed 300 'bad' websites and blogs."[48]

[42] "Internet Censorship Tightening in Vietnam," AsiaNews.it, June 22, 2010, http://www.asianews.it/news-en/Internet-censorship-tightening-in-Vietnam-18746.html.
[43] Phong Quan, "Sim Card Registration Now Required in Vietnam," *Vietnam Talking Points*, January 16, 2010, http://talk.onevietnam.org/sim-card-registration-now-required-in-vietnam/.
[44] Human Rights Watch, "Vietnam: Stop Cyber Attacks Against Online Critics."
[45] "Authorities Crush Online Dissent; Activists Detained Incommunicado," *Free News Free Speech* (blog), June 2, 2010, http://freenewsfreespeech.blogspot.com/2010/06/authorities-crush-online-dissent.html.
[46] George Kurtz, "Vietnamese Speakers Targeted in Cyberattack," *CTO* (blog), March 30, 2010, http://siblog.mcafee.com/cto/vietnamese-speakers-targeted-in-cyberattack/; Neel Mehta, "The Chilling Effect of Malware," *Google Online Security Blog*, March 30, 2010, http://googleonlinesecurity.blogspot.com/2010/03/chilling-effects-of-malware.html.
[47] Kurtz, "Vietnamese Speakers Targeted in Cyberattack."
[48] Human Rights Watch, "Vietnam: Stop Cyber Attacks Against Online Critics."

ZIMBABWE

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Partly Free**
Obstacles to Access	n/a	16
Limits on Content	n/a	15
Violations of User Rights	n/a	23
Total	**n/a**	**54**

POPULATION: 12.6 million
INTERNET PENETRATION: 11 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Internet and mobile-phone usage is nominally free from government interference in Zimbabwe, but there are indications that the government has a strong desire to control these communications technologies. There are also a number of practical obstacles that hinder citizens' access, including poor infrastructure in urban areas, and an almost total lack of infrastructure in rural areas. Over the past decade, the country has experienced a major economic decline, contributing to severe power shortages and accelerated deterioration of the telecommunications system.[1] Low bandwidth has also made internet connections extremely slow in Zimbabwe. Although internet access remains limited, since early 2009, the number of mobile-phone users has increased exponentially.[2]

The most worrisome development for the digital media sector has been the 2007 adoption of the Interception of Communications Act,[3] which allows the government to monitor postal, telephonic, and internet traffic, and requires service providers to intercept

[1] Zimbabwe's economy contracted significantly between 1999 and 2009 due to a political crisis associated with President Robert Mugabe's controversial land-reform campaign, which entailed seizing white-owned farms and distributing them to black loyalists. Inflation shot to astronomical rates of several billion percent, and the exchange rate of the Zimbabwean dollar tumbled to more than 50 billion per U.S. dollar. See BuddeComm, "Zimbabwe—Telecoms, Mobile, Broadband and Forecasts: Executive Summary," http://www.budde.com.au/Research/Zimbabwe-Telecoms-Mobile-Broadband-and-Forecasts.html, accessed August 18, 2010.

[2] "Zimbabwe Cell Phone Boom Still Can't Beat Investor Fears," My Broadband News, September 28, 2010, http://mybroadband.co.za/news/cellular/15445-Zimbabwe-cell-phone-boom-still-cant-beat-investor-fears.html. [3] The Interception of Communications Act is available at http://www.kubatana.net/docs/legisl/ica_070803.pdf, accessed August 22, 2010.

[3] The Interception of Communications Act is available at http://www.kubatana.net/docs/legisl/ica_070803.pdf, accessed August 22, 2010.

information on the state's behalf.[4] The regime has committed rampant human rights abuses and exercised strict control over the traditional media, but no concrete evidence of systematic internet filtering has been reported.[5] Nevertheless, with the spread of mobile phones and the use of text messages to disseminate information critical of President Robert Mugabe and his supporters, the authorities have imposed some content restrictions and registration requirements related to these technologies in recent years.

The internet was first introduced in Zimbabwe in 1997, following the establishment of the first internet-service provider (ISP), Data Control, in 1996. The medium's development has been rather uneven and erratic, owing to severe political and economic crises that have gripped the country since 2000.

OBSTACLES TO ACCESS

Internet access has expanded rapidly in Zimbabwe, from a penetration rate of 0.3 percent in 2000 to about 12 percent (or 1.4 million of the country's estimated 11.4 million people) by the end of 2009.[6] The mushrooming of cybercafes in most of the country's urban centers, coupled with the forced migration of many Zimbabweans to South Africa, the United Kingdom, Australia, and other countries as a result of the political and economic crisis, created a favorable environment for increased internet usage, as the new expatriates sought to stay in touch with friends and family in Zimbabwe. High prices and limited infrastructure put access to the internet beyond the reach of most of the population, particularly in rural areas. But for those who want to communicate with friends and relatives abroad, the internet represents a faster, easier, and cheaper alternative to telephony and postal services. Furthermore, the restrictive traditional media environment, which is dominated by state-owned outlets, has made the internet popular with citizens seeking alternative information.

There is a vast divide between urban and rural areas with respect to internet penetration. Most rural communities are geographically isolated and economically disadvantaged, and have consequently failed to attract the interest of commercial service providers. Telephone penetration in rural areas is minimal, with lack of electricity representing a major challenge; radio remains the main communication medium in such regions. Many rural telephone connections are still shared or "party" lines, leading to poor

[4] Nqobizitha Khumlo, "Zim Internet Service Providers Struggle to Buy Spying Equipment," Kubatana.net, August 10, 2007, http://www.kubatana.net/html/archive/inftec/070810zol1.asp?spec_code=060426commdex&sector=INFTEC&year=0&range_start=1&intMainYear=0&intTodayYear=2010.

[5] OpenNet Initiative, "Country Profile: Zimbabwe," September 30, 2009, http://opennet.net/research/profiles/zimbabwe.

[6] International Telecommunications Union (ITU), "ICT Statistics—Internet," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

or unreliable transmission quality, slow connection speeds, and difficulty initiating dial-up internet connections.[7]

Even in urban areas, electricity is regularly rationed, and the penetration of both the internet and mobile phones is uneven. In practice, internet access is limited largely to the few Zimbabweans with formal employment or positions in institutions of higher learning. There is little if any internet penetration in the poor townships surrounding cities, where much of the population lives, as few township residents can afford it. Internet penetration is highest in the central business districts of the country's two major cities, Bulawayo and Harare. However, with newly licensed data carriers starting to roll out fiber-optic networks across the country and establish links to international undersea cables, the situation is expected to improve.[8]

The prices for internet access in Zimbabwe are set by owners of cybercafes and ISPs; the state has so far not interfered on this issue. But with the majority of Zimbabweans surviving on wages of around US$1,800 per year, a cost of living of more than US$6,000 per year, and access prices set at some US$600 per year for one hour of usage per day, the internet in Zimbabwe is mainly for the affluent.[9] For those seeking home access, the general cost of a computer is US$1,300, a modem costs US$175, and the annual local telephone charges for dial-up access are around US$208.[10] Fast and reliable satellite connections to the internet are also very expensive. Even those who have access to the internet at work can only use it for a limited amount of time, as companies seek to contain the high monthly fees they pay for broadband.

Mobile-phone penetration is far higher than internet penetration, at almost 50 percent of the population (more than five million people) as of September 2010, an increase from 9 percent in early 2009.[11] Econet Wireless introduced third-generation (3G) technology in July 2009 and fourth-generation (4G) technology in May 2010, after two years of waiting for an allocation of frequencies by the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ). Given the monthly subscription fee of US$25, the 3G service is only affordable for the few who are still gainfully employed in a country where the jobless rate is estimated at 94 percent.[12] In fact, some observers fear that

[7] Zimbabwe has one fixed-line telephone operator, the publicly owned TelOne (formerly the Posts and Telecommunications Corporation, or PTC), which has failed to provide universal access. TelOne boasts just 386,000 subscribers, 50 percent of whom are in the capital, Harare. Only 17 percent of the lines are in rural areas, and 92 percent of the total lines have been digitalized. See "An Overview of Zimbabwe's Telecommunications—Potraz Presentation Download," *Technology Zimbabwe* (blog), March 5, 2010, http://www.techzim.co.zw/2010/03/zimbabwe-telecoms-overview/.

[8] BuddeComm, "Zimbabwe."

[9] OpenNet Initiative, "Country Profile: Zimbabwe"; "Review: Ecoweb's 4G Mobile WiMax," *Technology Zimbabwe*, May 30, 2010, http://www.techzim.co.zw/2010/05/review-ecoweb-4g-mobile-wimax/.

[10] Getrude Gumede, "Websites for Zimbabwean Cabinet Ministries," *Zimbabwe Telegraph*, July 2, 2009, http://www.zimtelegraph.com/?p=1249.

[11] BuddeComm, "Zimbabwe."; "Zimbabwe Cell Phone Boom Still Can't Beat Investor Fears."

[12] UN Central Emergency Response Fund, "CERF Allocates $5 Million for Protracted Relief and Recovery Operation in Zimbabwe," news release, January 14, 2010, http://ochaonline.un.org/CERFaroundtheWorld/Zimbabwe2010/tabid/6430/language/en-US/Default.aspx.

rather than enhancing access to the internet for the general public, advanced mobile-phone service may sharpen the digital divide by improving access for the few who already have it. Because of inadequate infrastructural development, the current 3G internet is frustratingly slow. 4G mobile internet access is even more expensive. Initial equipment costs about US$175, and the current monthly subscription stands at US$115 per month.[13] The rate for pre-paid mobile web access is US$0.20 per megabyte, with "bundles" ranging from 1 to 1000 megabytes.[14] Despite the high costs, during the first week of re-launching its mobile broadband package in October 2010, Econet reported 100,000 new subscribers, and the number continued to grow through to year's end.[15]

Dial-up internet services have been negatively affected by the collapse of the landline infrastructure, with the state-owned telecommunications firm TelOne failing to upgrade or repair its network. Broadband in Zimbabwe consists mainly of direct satellite connections through VSAT. Other access technologies include GSM, WiMax, and fiber-optic or copper-wire ADSL. Broadband is available in major urban areas, particularly in Harare, Bulawayo, and Mutare, and there are plans to extend coverage to other cities.[16] However, in addition to the prohibitive cost, broadband is still very slow at 256 kbps. It is largely used by companies, nongovernmental organizations (NGOs), and universities, as most households cannot afford it. The cost of broadband is expected to fall when Econet finishes laying fiber optic cables in late 2010.

Although there is no clear evidence that the government blocks access to digital media, there are structural constraints that suggest indirect blocking. For instance, it is a requirement for every ISP to allow the government to monitor certain traffic at any given time, and all licensed ISPs must connect through the limited internet-access provider (IAP) infrastructure. The government has allocated few frequencies to IAPs, which require expensive equipment. For those who are able to get online, social-networking, video-sharing, and microblogging sites such as Facebook, YouTube, and Twitter are freely available, as are international blog-hosting platforms.

ISPs and mobile-phone companies are licensed and regulated by POTRAZ, whose leaders are appointed by the president in consultation with the minister of transport and communication. POTRAZ has been widely accused of partisanship and making politicized decisions, such as the cancellation of TeleAccess's operating license in 2005.[17] The regulator has not directly blocked the establishment of ISPs, but the exorbitant application fees it

[13] "Review: Ecoweb's 4G Mobile WiMax," *Technology Zimbabwe*.
[14] "Mobile Internet Revolution Takes Zimbabwe by Storm," The Zimbabwean, October 27, 2010, http://www.thezimbabwean.co.uk/index.php?option=com_content&view=article&id=35162:mobile-internet-revolution-takes-zimbabwe-by-storm&catid=69:sunday-top-stories&Itemid=30.
[15] "Econet Connects 100,000 to Internet," Bulawayo, http://bulawayoonline.com/latest-news/econet-connects-100-000-to-internet.html, accessed March 5, 2011.
[16] See GlobalTT.com, "Zimbabwe," http://www.globaltt.com/coverage_countries/Zimbabwe, accessed August 25, 2010.
[17] "Potraz Just Playing Dirty Politics—Shumba," *Zimbabwe Independent*, November 18, 2005, http://www.theindependent.co.zw/business/13372.html.

charges have hindered the proliferation of such businesses. The fees for IAPs and ISPs range from US$2 million to US$4 million, depending on the type of service to be provided. This is in addition to the 3.5 percent of annual gross income that the provider must pay to POTRAZ.[18] Application fees for operating a mobile-phone service are equally steep. There are currently 12 licensed IAPs and 17 ISPs in Zimbabwe.[19] Only one of the IAPs, CommIT, has a Class B license, which entitles it to offer internet-based voice services in addition to the normal services that the rest provide.[20] Before the IAPs install their equipment, it has to be vetted and approved by the regulator. In addition, the Post and Telecommunications Act of 2000 requires that ISPs renew contracts with TelOne for access to its fixed-line network. However, there are no stringent regulations that hinder the establishment of cybercafes.

LIMITS ON CONTENT

Despite reports of continued human rights abuses and government control over the traditional media, there has been no concrete evidence of systematic internet filtering in Zimbabwe. However, some instances of surveillance and censorship have been reported. For example, in previous years, e-mail messages to central bank employees were allegedly blocked if they contained references to the main opposition party, the Movement for Democratic Change (MDC), or its leader, Morgan Tsvangirai. There have also been cases in which the authorities apparently traced antigovernment e-mail content to its source and arrested suspected senders.[21]

The government has from time to time exhibited a desire to control mobile-phone communications, for instance by warning operators not to let subscribers use their networks for political purposes, especially during elections or in other potentially volatile situations. The authorities issued such a warning in response to the mass circulation of text messages castigating the ruling Zimbabwean African National Union–Patriotic Front (ZANU-PF) during its December 2009 party congress. Econet has in turn warned all its subscribers that their service would be cut off if they sent political messages.[22] In June 2010, just days after a column in the government-controlled *Herald* newspaper threatened Econet with the loss of its operating license, the company complained to the MDC about its use of the network for political purposes, and announced that it was installing software that would identify and block problematic messages.

[18] The POTRAZ website can be found at http://www.potraz.gov.zw/.
[19] "An Overview of Zimbabwe's Telecommunications—Potraz Presentation Download," *Technology Zimbabwe*.
[20] "POTRAZ Calls ICT Providers to Help Define IAP/ISP Roles," *Technology Zimbabwe*, May 6, 2010, http://www.techzim.co.zw/2010/05/potraz-iap-isp-roles/.
[21] OpenNet Initiative, "Zimbabwe."
[22] "Zanu PF Texts Sent from Sweden: Econet," *New Zimbabwe*, December 17, 2009, http://www.newzimbabwe.com/news-1491-Zanu+PF+texts+sent+from+Sweden/news.aspx.

The various obstacles to access in Zimbabwe limit the utility of the internet as a means of mass mobilization. Even within the fraction of the population that accesses the medium regularly, there is no coordinated use of social-networking sites to build support for political change. However, overseas-based independent news websites and other digital media have emerged as an important source of alternative information for those able to access them. Sites such as www.newzimbabwe.com and www.zimonline.co.za publish independent information often obtained from stringers or other contacts based inside Zimbabwe, at times generating news later picked up by mainstream media outlets. Thus, during the hotly contested 2008 elections, Zimbabweans used mobile-phone text messages and blogs to disseminate oppositionist and independent versions of events that were not addressed in the severely restricted traditional media. Civic organizations such as Kubatana have been using specialized software to disseminate bulk political text messages to their subscribers and receive feedback from them.[23] By contrast, sites like Facebook are mainly used for friendly chats and renewing lapsed social contacts, possibly because of the lack of anonymity on such sites, and fear of repercussions if politically-oriented statements are traced back to those expressing them. Debates on the country's political and socioeconomic issues and reactions to internet stories on Zimbabwe are mostly confined to chat rooms and feedback sections of online news sites. Even in those cases, the base of contributors is fairly narrow, and the quality of the discussion is often poor.

Blogging offers community organizations, minorities, and individuals the opportunity to express their views, but few internet users know how to establish a blog or have sufficient access to properly maintain one. While some journalists have had training on creating blogs and using various internet tools, they have only rarely shown both the desire and the practical ability to sustain their own sites. Many individuals blogging from inside the country publish under their own names even when harshly criticizing the government, though some retain anonymity for fear of reprisals. Though their overall number is relatively small, blogs have nevertheless become critically important in Zimbabwe as an alternative space for debate, particularly due to the large number of bloggers based outside of the country.

VIOLATIONS OF USER RIGHTS

The constitution provides for freedom of expression, including freedom from interference with personal correspondence. However, Section 20(2) of the constitution places a number of limitations on these rights in the interests of national defense, public safety, public order, public morality, public health, and town or country planning.[24] Currently, there are no laws

[23] Ken Banks, "Mobile Phones Play Role in Zimbabwe," *PCWorld*, April 14, 2008, http://www.pcworld.com/businesscenter/article/144535/mobile_phones_play_role_in_zimbabwe.html.
[24] The text of the constitution is available at http://www.parlzim.gov.zw/cms/UsefulResourses/ZimbabweConstitution.pdf.

that specifically protect online modes of communication. Bloggers are not recognized by law as eligible for accreditation as journalists.

Judicial independence is compromised by an appointment process that allows for high levels of executive interference. The judiciary has sometimes demonstrated a degree of autonomy through rulings that are not necessarily favorable to the state, including on freedom of expression, but the government often ignores such decisions.

While most of the charges against journalists in the past few years have either been withdrawn or have resulted in acquittals, continuous harassment of journalists by the authorities has often induced self-censorship, even among those writing for online publications. The country's civil and criminal defamation laws, the Interception of Communications Act (ICA), and the Criminal Law Codification and Reform Act (CODE) all apply equally to online journalists and reporters for traditional media.

The CODE punishes anyone who publicly undermines the authority of or insults the president in any printed or electronic medium with up to 20 years in prison.[25] In one recent case, business executive John Norman Alfred Rusthon was arrested in March 2010 for allegedly circulating an e-mail message with photographs purporting to show the lavish interior of the president's house. He was charged with undermining the office of the president under Section 33(2) (a)(i) of the CODE, and was released on US$200 bail several days later.[26] The case was apparently still pending as of the end of 2010.

The CODE has also been applied to internet-related activities outside Zimbabwe. For example, Andrew Meldrum, an American journalist writing for Britain's *Guardian* newspaper, was prosecuted in Zimbabwe in 2002 on charges of abusing journalistic privilege by publishing falsehoods on the paper's website. Prosecutors took the position that Zimbabwean courts have jurisdiction over content published on the internet so long as it can be accessed in Zimbabwe. Meldrum was acquitted, but immediately received a deportation order. Another judge then ruled that he had legal status to stay in the country, since he held a permanent residency permit. Nevertheless, he was reportedly abducted by state authorities in May 2003 and expelled to South Africa.[27]

Website owners, bloggers, and internet users in general are not required to register with the government. However, a July 2010 POTRAZ directive called for all mobile-phone users to register with the government by the end of August 2010, ostensibly to combat crime and threatening or obscene messages or calls.[28] In September, POTRAZ announced

[25] The law is available at http://www.kubatana.net/docs/legisl/criminal_law_code_050603.pdf.
[26] "Manager Arrested for Insulting the President," *Herald* (Zimbabwe), March 2, 2010, available at http://allafrica.com/stories/201003020057.html.
[27] "Andrew Meldrum's Video Diary," *Guardian*, http://www.guardian.co.uk/zimbabwe/subsectionmenu/0,,960624,00.html; Dave Gilson, "Hoping Against Hope: An Interview with Andrew Meldrum," *Mother Jones*, June 28, 2005, http://motherjones.com/politics/2005/06/hoping-against-hope-interview-andrew-meldrum.
[28] "Zim to Register Cell Phone Lines," *Southern Times*, June 21, 2010, http://www.southerntimesafrica.com/article.php?title=Zim%20to%20register%20cell%20phone%20lines%20%20&id=4290&sid=ba3950cf283bab09bb9dc934b7836a1c.

an indefinite extension of the deadline as it became clear that many users had been unable to register in time.[29]

The Post and Telecommunications Act of 2000 allows the government to monitor e-mail usage and requires ISPs to supply information to government officials when requested. The law obliges ISPs to report any e-mail with "offensive or dangerous" content. The Interception of Communications Act of 2007 (ICA) enabled the establishment of a monitoring center to oversee, among other things, traffic in all telecommunications and postal services.[30] The law requires telecommunications operators and ISPs to install the necessary technology at their own expense. Failure to comply can be punished with a fine or up to three years in prison. There have been unconfirmed reports that the government has received surveillance technology and training from China.[31]

The ICA allows the state to intercept any communication when there is a reasonable suspicion of threats to public safety or national security, among other situations. Intercepted information can in some instances be used as evidence in criminal proceedings. While there are no specific laws regulating the encryption of documents or communications, the ICA allows the government to request any key or code necessary to make a communication readable once there is reasonable suspicion that, for example, national security is at stake and an administrative warrant has been granted.

Warrants allowing monitoring and interception of communications are issued by the minister of information at his discretion, meaning there is no substantial judicial oversight or other independent safeguards against abuse. The frequency and extent of monitoring in practice remains uncertain.

There have been no known cases of physical attacks against bloggers or online journalists in particular, but they remain at risk in Zimbabwe's general climate of political violence and impunity. In 2006, then security minister Didymus Mutasa warned that the authorities would "soon close in on" journalists using pseudonyms to report in the exiled private media, including websites and internet radio stations.[32] Similarly, while many NGO activists and human rights defenders have been targeted by the regime, there are no known cases of such figures being physically harassed in relation to online or text-messaging activities.

[29] "Telecoms Regulator in Zimbabwe Extends Cell Phone Registration Exercise," Net News Publisher, September 1, 2010, http://www.netnewspublisher.com/telecoms-regulator-in-zimbabwe-extends-cell-phone-registration-exercise/.
[30] The law is available at http://kubatana.net/docs/legisl/icb_070508.pdf.
[31] Lance Guma, "Too Much to Monitor for Snooping Squads," SW Radio Africa, August 7, 2007, http://www.swradioafrica.com/news070807/snoop070807.htm; Reporters Without Borders, "All Communications Can Now Be Intercepted under New Law Signed by Mugabe," news release, August 6, 2007, http://en.rsf.org/zimbabwe-all-communications-can-now-be-06-08-2007,17623.html.
[32] Media Monitoring Project Zimbabwe (MMPZ), "Government Continues to Threaten Journalists," from *Weekly Media Update 2006*, no. 4 (January 23–29, 2006), available at Kubatana.net, http://www.kubatana.net/html/archive/media/060202mmpz1.asp?sector=MEDIA.

The websites of both government-controlled and private media have been hacked, but not on a large scale or with great frequency. The government has reportedly used Chinese assistance to bolster its efforts to instigate such attacks against opposition-oriented websites.

METHODOLOGY

This second edition of *Freedom on the Net* provides analytical reports and numerical ratings for 37 countries worldwide. The countries were chosen to provide a representative sample with regards to geographical diversity and economic development, as well as varying levels of political and media freedom. The ratings and reports included in this study particularly focus on developments that took place between January 1, 2009 and December 31, 2010.

WHAT WE MEASURE

The *Freedom on the Net* index aims to measure each country's level of internet and digital media freedom based on a set of methodology questions described below (see "Checklist of Questions"). Given increasing technological convergence, the index also measures access and openness of other digital means of transmitting information, particularly mobile phones and text messaging services.

Freedom House does not maintain a culture-bound view of freedom. The project methodology is grounded in basic standards of free expression, derived in large measure from Article 19 of the Universal Declaration of Human Rights:

> *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media regardless of frontiers."*

This standard applies to all countries and territories, irrespective of geographical location, ethnic or religious composition, or level of economic development.

The project particularly focuses on the transmission and exchange of news and other politically relevant communications, as well as the protection of users' rights to privacy and freedom from both legal and extralegal repercussions arising from their online activities. At the same time, the index acknowledges that in some instances freedom of expression and access to information may be legitimately restricted. The standard for such restrictions applied in this index is that they be implemented only in narrowly defined circumstances and in line with international human rights standards, the rule of law, and the principles of necessity and proportionality. As much as possible, censorship and surveillance policies and procedures should be transparent and include avenues for appeal available to those affected.

The index does not rate governments or government performance per se, but rather the real-world rights and freedoms enjoyed by individuals within each country. While digital

media freedom may be primarily affected by state actions, pressures and attacks by nonstate actors, including the criminal underworld, are also considered. Thus, the index ratings generally reflect the interplay of a variety of actors, both governmental and nongovernmental, including private corporations.

THE SCORING PROCESS

The index aims to capture the entire "enabling environment" for internet freedom within each country through a set of 21 methodology questions, divided into three subcategories, which are intended to highlight the vast array of relevant issues. Each individual question is scored on a varying range of points. Assigning numerical points allows for comparative analysis among the countries surveyed and facilitates an examination of trends over time. Countries are given a total score from 0 (best) to 100 (worst) as well as a score for each subcategory. Countries scoring between 0 to 30 points overall are regarded as having a "Free" internet and digital media environment; 31 to 60, "Partly Free"; and 61 to 100, "Not Free". An accompanying country report provides narrative detail on the points covered by the methodology questions.

The methodology examines the level of internet freedom through a set of 21 questions and nearly 100 accompanying subpoints, organized into three groupings:

- ***Obstacles to Access***—including infrastructural and economic barriers to access; governmental efforts to block specific applications or technologies; legal and ownership control over internet and mobile phone access providers.
- ***Limits on Content***—including filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism.
- ***Violations of User Rights***—including legal protections and restrictions on online activity; surveillance and limits on privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.

The purpose of the subpoints is to guide analysts regarding factors they should consider while evaluating and assigning the score for each methodology question. After researchers submitted their draft scores, Freedom House convened three regional review meetings and several international conference calls, attended by Freedom House staff and a range of local experts, scholars, and civil society representatives from the countries under study. During the meetings, participants reviewed, critiqued, and adjusted the draft scores through careful consideration of events, laws, and practices relevant to each item. After

completing the regional and country consultations, Freedom House staff did a final review of all scores to ensure their comparative reliability and integrity.

**** Note on changes from 2009 pilot edition***

Freedom House released a pilot edition of *Freedom on the Net* in April 2009, assessing a sample of 15 countries. Following the report's publication and drawing on feedback from a range of audiences, including analysts and academic advisers involved in production of the pilot study, Freedom House staff made several modifications to the methodology. In particular, question B1 on censorship and question C7 on attacks were each split into two separate questions in order to clarify and sharpen the analytical rigor with which obstacles to internet freedom are identified. In addition, in order to retain the accuracy of score comparisons between the pilot edition and this study, for those countries included in both, a number of minor adjustments were made to the 2009 scores on the basis of updated scoring guidelines used for the 2011 edition. In the present edition, the adjusted 2009 scores are presented in order to best convey changes over time in each country assessed.

CHECKLIST OF QUESTIONS

- Each country is ranked on a scale of 0 to 100, with 0 being the best and 100 being the worst.
- A combined score of 0-30=Free, 31-60=Partly Free, 61-100=Not Free.
- Under each question, **a lower number of points is allotted for a more free situation, while a higher number of points is allotted for a less free environment.**
- Unless otherwise indicated, the sub-questions listed are meant to provide guidance as to what Issues should be addressed under each methodology question, though not all will apply to every country.

A. OBSTACLES TO ACCESS (0-25 POINTS)

1. **To what extent do infrastructural limitations restrict access to the internet and other ICTs? (0-6 points)**
   - *Does poor infrastructure (electricity, telecommunications, etc) limit citizens' ability to receive internet in their homes and businesses?*
   - *To what extent is there widespread public access to the internet through internet cafes, libraries, schools and other venues?*
   - *To what extent is there internet and mobile phone access, including via 3G networks or satellite?*
   - *Is there a significant difference between internet and mobile-phone penetration and access in rural versus urban areas or across other geographical divisions?*
   - *To what extent are broadband services widely available in addition to dial-up?*

2. **Is access to the internet and other ICTs prohibitively expensive or beyond the reach of certain segments of the population? (0-3 points)**
   - *In countries where the state sets the price of internet access, is it prohibitively high?*
   - *Do financial constraints, such as high costs of telephone/internet services or excessive taxes imposed on such services, make internet access prohibitively expensive for large segments of the population?*
   - *Do low literacy rates (linguistic and "computer literacy") limit citizens' ability to use the internet?*
   - *Is there a significant difference between internet penetration and access across ethnic or socio-economic societal divisions?*
   - *To what extent are online software, news, and other information available in the main local languages spoken in the country?*

3. **Does the government impose restrictions on ICT connectivity and access to particular Web 2.0 applications permanently or during specific events? (0-6 points)**
   - *Does the government place limits on the amount of bandwidth that access providers can supply?*
   - *Does the government use control over internet infrastructure (routers, switches, etc.) to limit connectivity, permanently or during specific events?*
   - *Does the government centralize telecommunications infrastructure in a manner that could facilitate control of content and surveillance?*
   - *Does the government block protocols and tools that allow for instant, person-to-person communication (VOIP, instant messaging, text messaging, etc.), particularly those based outside the country (i.e. YouTube, Facebook, Skype, etc.)?*
   - *Does the government block protocols and Web 2.0 applications that allow for information sharing or building online communities (video-sharing, social-networking sites, comment features, blogging platforms, etc.) permanently or during specific events?*
   - *Is there blocking of certain tools that enable circumvention of online filters and censors?*

4. **Are there legal, regulatory, or economic obstacles that prevent the existence of diverse business entities providing access to digital technologies? (0-6 points)**

   Note: Each of the following access providers are scored separately:

   1a. Internet-service providers (ISPs) and other backbone internet providers (0-2 points)
   1b. Cybercafes and other businesses that allow public internet access (0-2 points)
   1c. Mobile phone companies (0-2 points)

   - *Is there a legal or de facto monopoly over access providers or do users have a choice of access provider, including ones privately owned?*
   - *Is it legally possible to establish a private access provider or does the state place extensive legal or regulatory controls over the establishment of providers?*
   - *Are registration requirements (e.g. bureaucratic "red tape") for establishing an access provider unduly onerous or are they approved/rejected on partisan or prejudicial grounds?*
   - *Does the state place prohibitively high fees on the establishment and operation of access providers?*

5. **To what extent do national regulatory bodies overseeing digital technology operate in a free, fair, and independent manner? (0-4 points)**
   - *Are there explicit legal guarantees protecting the independence and autonomy of any regulatory body overseeing internet and other ICTs (exclusively or as part of a broader mandate) from political or commercial interference?*
   - *Is the process for appointing members of regulatory bodies transparent and representative of different stakeholders' interests?*
   - *Are decisions taken by the regulatory body, particularly those relating to ICTs, seen to be fair and apolitical and to take meaningful notice of comments from stakeholders in society?*

- *Are efforts by access providers and other internet-related organizations to establish self-regulatory mechanisms permitted and encouraged?*
- *Does the allocation of digital resources, such as domain names or IP addresses, on a national level by a government-controlled body create an obstacle to access or are they allocated in a discriminatory manner?*

B. LIMITS ON CONTENT (0-35 POINTS)

1. **To what extent does the state or other actors block or filter internet and other ICT content, particularly on political and social issues? (0-6 points)**
   - *Is there significant blocking or filtering of internet sites, web pages, blogs, or data centers, particularly those related to political and social topics?*
   - *Is there significant filtering of text messages or other content transmitted via mobile phones?*
   - *Do state authorities block or filter information and views from inside the country—particularly concerning human rights abuses, government corruption, and poor standards of living—from reaching the outside world through interception of e-mail or text messages, etc?*
   - *Are methods such as deep-packet inspection used for the purposes of preventing users from accessing certain content or for altering the content of communications en route to the recipient, particularly with regards to political and social topics?*

2. **To what extent does the state employ legal, administrative, or other means to force deletion of particular content, including requiring private access providers to do so? (0-4 points)**
   - *To what extent are non-technical measures—judicial or extra-legal—used to order the deletion of content from the internet, either prior to or after its publication?*
   - *To what degree does the government or other powerful political actors pressure or coerce online news outlets to exclude certain information from their reporting?*
   - *Are access providers and content hosts legally responsible for the information transmitted via the technology they supply or required to censor the content accessed or transmitted by their users?*
   - *Are access providers or content hosts prosecuted for opinions expressed by third parties via the technology they supply?*

3. **To what extent are restrictions on internet and ICT content transparent, proportional to the stated aims, and accompanied by an independent appeals process? (0-4 points)**
   - *Are there national laws, independent oversight bodies, and other democratically accountable procedures in place to ensure that decisions to restrict access to certain content are proportional to their stated aim?*
   - *Are state authorities transparent about what content is blocked or deleted (both at the level of public policy and at the moment the censorship occurs)?*
   - *Do state authorities block more types of content than they publicly declare?*

- *Do independent avenues of appeal exist for those who find content they produced to have been subjected to censorship?*

4. Do online journalists, commentators, and ordinary users practice self-censorship? (0-4 points)

- *Is there widespread self-censorship by online journalists, commentators, and ordinary users in state-run online media, privately run websites, or social media applications?*
- *Are there unspoken "rules" that prevent an online journalist or user from expressing certain opinions in ICT communication?*
- *Is there avoidance of subjects that can clearly lead to harm to the author or result in almost certain censorship?*

5. To what extent is the content of online sources of information determined or manipulated by the government or a particular partisan interest? (0-4 points)

- *To what degree do the government or other powerful actors pressure or coerce online news outlets to follow a particular editorial direction in their reporting?*
- *Do authorities issue official guidelines or directives on coverage to online media outlets, blogs, etc., including instructions to marginalize or amplify certain comments or topics for discussion?*
- *Do government officials or other actors bribe or use close economic ties with online journalists, bloggers, website owners, or service providers in order to influence the online content they produce or host?*
- *Does the government employ, or encourage content providers to employ, individuals to post pro-government remarks in online bulletin boards and chat rooms?*
- *Do online versions of state-run or partisan traditional media outlets dominate the online news landscape?*

6. Are there economic constraints that negatively impact users' ability to publish content online or online media outlets' ability to remain financially sustainable? (0-3 points)

- *Are favorable connections with government officials necessary for online media outlets or service providers (e.g. search engines, e-mail applications, blog hosting platforms, etc.) to be economically viable?*
- *Are service providers who refuse to follow state-imposed directives to restrict content subject to sanctions that negatively impact their financial viability?*
- *Does the state limit the ability of online media to accept advertising or investment, particularly from foreign sources, or does it limit advertisers from conducting business with disfavored online media or service providers?*
- *To what extent do ISPs manage network traffic and bandwidth availability to users in a manner that is transparent, evenly applied, and does not discriminate against users or producers of content based on the content/source of the communication itself (i.e. respect "net neutrality" with regard to content)?*
- *To what extent do users have access to free or low-costs blogging services, webhosts, etc. to allow them to make use of the internet to express their own views?*

7. **To what extent are sources of information that are robust and reflect a diversity of viewpoints readily available to citizens, despite government efforts to limit access to certain content? (0-4 points)**
   - *Are people able to access a range of local and international news sources via the internet or text messages, despite efforts to restrict the flow of information?*
   - *Does the public have ready access to media outlets or websites that express independent, balanced views?*
   - *Does the public have ready access to sources of information that represent a range of political and social viewpoints?*
   - *To what extent do online media outlets and blogs represent diverse interests within society, for example through websites run by community organizations or religious, ethnic and other minorities?*
   - *To what extent do users employ proxy servers and other methods to circumvent state censorship efforts?*

8. **To what extent do individuals use the internet and other ICT technologies as sources of information and tools for mobilization, particularly regarding political and social issues? (0-6 points)**
   - *Are internet sources (news websites, blogs, etc) a primary medium of news dissemination for a large percentage of the population?*
   - *To what extent does the online community cover political developments and provide scrutiny of government policies, official corruption, or actions by other powerful societal actors?*
   - *To what extent are online communication (e.g. Twitter) or social networking sites (e.g. Facebook, Orkut) used as a means to organize politically, including for "real-life" activities?*
   - *Are cell phones and ICTs used as a medium of news dissemination and political organization, including on otherwise banned topics?*

C. VIOLATIONS OF USER RIGHTS (0-40 POINTS)

1. **To what extent does the constitution or other laws contain provisions designed to protect freedom of expression, including on the internet, and are they enforced? (0-6 points)**
   - *Does the constitution contain language that provides for freedom of speech and of the press generally?*
   - *Are there laws or legal decisions that specifically protect online modes of expression?*
   - *Are online journalists and bloggers accorded the same rights and protections given to print and broadcast journalists?*
   - *Is the judiciary independent and do the Supreme Court, Attorney General, and other representatives of the higher judiciary support free expression?*
   - *Is there implicit impunity for private and/or state actors who commit crimes against online journalists, bloggers, or other citizens targeted for their online activities?*

2. **Are there laws which call for criminal penalties or civil liability for online and ICT activities? (0-4 points)**
   - *Are there specific laws criminalizing online expression and activity such as posting or downloading information, sending an e-mail, or text message, etc.? (Note: this excludes legislation addressing harmful content such as child pornography or activities such as malicious hacking)*
   - *Do laws restrict the type of material that can be communicated in online expression or via text messages, such as communications about ethnic or religious issues, national security, or other sensitive topics?*
   - *Are restrictions of internet freedom closely defined, narrowly circumscribed, and proportional to the legitimate aim?*
   - *Are vaguely worded penal codes or security laws applied to internet-related or ICT activities?*
   - *Are there penalties for libeling officials or the state in online content?*
   - *Can an online outlet based in another country be sued if its content can be accessed from within the country (i.e. "libel tourism")?*

3. **Are individuals detained, prosecuted or sanctioned by law enforcement agencies for disseminating or accessing information on the internet or via other ICTs, particularly on political and social issues? (0-6 points)**
   - *Are writers, commentators, or bloggers subject to imprisonment or other legal sanction as a result of posting material on the internet?*
   - *Are citizens subject to imprisonment, civil liability, or other legal sanction as a result of accessing or downloading material from the internet or for transmitting information via e-mail or text messages?*
   - *Does the lack of an independent judiciary or other limitations on adherence to the rule of law hinder fair proceedings in ICT-related cases?*
   - *Are individuals subject to abduction or arbitrary detention as a result of online activities, including membership in certain online communities?*
   - *Are penalties for "irresponsible journalism" or "rumor mongering" applied widely?*
   - *Are online journalists, bloggers, or others regularly prosecuted, jailed, or fined for libel or defamation (including in cases of "libel tourism")?*

4. **Does the government place restrictions on anonymous communication or require user registration? (0-4 points)**
   - *Are website owners, bloggers, or users in general required to register with the government?*
   - *Are users able to post comments online or purchase mobile phones anonymously or does the government require that they use their real names or register with the government?*
   - *Are users prohibited from using encryption software to protect their communications?*
   - *Are there laws restricting the use of encryption and other security tools, or requiring that the government be given access to encryption keys and algorithms?*

5. **To what extent is there state surveillance of internet and ICT activities without judicial or other independent oversight, including systematic retention of user traffic data? (0-6 points)**
   - *Do the authorities regularly monitor websites, blogs, and chat rooms, or the content of e-mail and mobile text messages, including via deep-packet inspection?*
   - *To what extent are restrictions on the privacy of digital media users transparent, proportional to the stated aims, and accompanied by an independent process for lodging complaints of violations?*
   - *Where the judiciary is independent, are there procedures in place for judicial oversight of surveillance and to what extent are these followed?*
   - *Where the judiciary lacks independence, is there another independent oversight body in place to guard against abusive use of surveillance technology and to what extent is it able to carry out its responsibilities free of government interference?*
   - *Is content intercepted during internet surveillance admissible in court or has it been used to convict users in cases involving free speech?*

6. **To what extent are providers of access to digital technologies required to aid the government in monitoring the communications of their users? (0-6 points)**

   Note: Each of the following access providers are scored separately:

   1a. Internet-service providers (ISPs) and other backbone internet providers (0-2 points)
   1b. Cybercafes and other businesses that allow public internet access (0-2 points)
   1c. Mobile phone companies (0-2 points)

   - *Are access providers required to monitor their users and supply information about their digital activities to the government (either through technical interception or via manual monitoring, such as user registration in cybercafes)?*
   - *Are access providers prosecuted for not doing so?*
   - *Does the state attempt to control access providers through less formal methods, such as codes of conduct?*
   - *Can the government obtain information about users without a legal process?*

7. **Are bloggers, other ICT users, websites, or their property subject to extralegal intimidation or physical violence by state authorities or any other actor? (0–5 points)**
   - *Are individuals subject to murder, beatings, harassment, threats, travel restrictions, or torture as a result of online activities, including membership in certain online communities?*
   - *Do armed militias, organized crime elements, insurgent groups, political or religious extremists, or other organizations regularly target online commentators?*
   - *Have online journalists, bloggers, or others fled the country or gone into hiding to avoid such action?*
   - *Have cybercafes or property of online commentators been targets of physical attacks or the confiscation or destruction of property as retribution for online activities or expression?*

8. **Are websites, governmental and private entities, ICT users, or service providers subject to widespread "technical violence," including cyberattacks, hacking, and other malicious threats? (0-3 points)**
   - *Are financial, commercial, and governmental entities subject to significant and targeted cyberattacks (e.g. cyber espionage, data gathering, DoS attacks), including those originating from outside of the country?*
   - *Have websites belonging to opposition or civil society groups within the country's boundaries been temporarily or permanently disabled due to cyberattacks, particularly at politically sensitive times?*
   - *Are websites or blogs subject to targeted technical attacks as retribution for posting certain content (e.g. on political and social topics)?*
   - *Are laws and policies in place to prevent and protect against cyberattacks (including the launching of systematic attacks by non-state actors from within the country's borders) and are they enforced?*

CONTRIBUTORS

FREEDOM HOUSE STAFF

- Sanja Kelly, Senior Researcher and Managing Editor, Freedom House
- Sarah Cook, Asia Analyst and Assistant Editor, Freedom House

REPORT AUTHORS AND ADVISORS

- **Australia:** Alana Maurushat, Academic Director, Cyberspace Law and Policy Centre, University of New South Wales
- **Brazil:** Carolina Rossini, attorney and coordinator for the Brazilian Open Educational Resources Project
- **Burma**: Min Zin, Burmese journalist and graduate student in political science at the University of California, Berkeley
- **China** (Advisor)**:** Xiao Qiang, Director of China Internet Project and an adjunct professor, Graduate School of Journalism, University of California, Berkeley
- **Cuba:** Ernesto Hernández Busto, blogger and journalist based in Spain
- **Estonia:** Linnar Viik, information society expert and Rector, Estonian IT College
- **Georgia:** Giorgi (Giga) Paitchadze, founder of Georgian New Media Institute
- **Germany:** Heike Jensen, lecturer at the Department of Gender Studies of Humboldt University, Berlin
- **India:** Ketan Tanna, Feature and Web Editor, *The Free Press Journal*, Mumbai
- **Iran:** Mahmood Enayat, Director, Iran Media Program, Annenberg School of Communication, University of Pennsylvania
- **Italy:** Giampiero Giacomello, Assistant Professor of International Relations, University of Bologna
- **Jordan:** Sa'eda Kilani, Founder and General Director, Arab Archives Institute, Amman

- **Kazakhstan**: Yelena Jetpyspayeva, consultant and Managing Editor, NewEurasia.net
- **Kenya:** Ory Okolloh, lawyer, blogger, and co-founder of Ushahidi
- **Mexico:** Alejandra Ezeta, Executive Director, Ciudadanos en Medios: Democracia e Información
- **Nigeria:** 'Gbenga Sesan, Executive Director, Paradigm Initiative Nigeria
- **Russia:** Alexey Sidorenko, Managing Editor, RuNet Project at Global Voices Online
- **South Africa:** Jane Duncan, Highway Africa Chair of Media and Information Society, School of Journalism and Media Studies, Rhodes University
- **Southeast Asia** (Advisor): Bridget Welsh, Associate Professor in Political Science, Singapore Management University
- **South Korea:** Yenn Lee, Ph.D. Politics Department, Royal Holloway, University of London
- **Thailand:** Supinya Klangnarong, Vice-Chair, Campaign for Popular Media Reform and Board Member of Thai Netizen Network
- **Turkey:** Yaman Akdeniz, Associate Professor of Law, Istanbul Bilgi University and founder of Cyber-Rights.org
- **United Kingdom**: David Banisar, Senior Legal Counsel for Article 19, London
- **United States**: Lauren Gelman, lecturer at Stanford Law School and founder of the consulting firm BlurryEdge Strategies in San Francisco

The analysts for the reports on Azerbaijan, Bahrain, Belarus, China, Egypt, Ethiopia, Indonesia, Malaysia, Pakistan, Rwanda, Saudi Arabia, Tunisia, Venezuela, Vietnam and Zimbabwe are independent internet researchers who have requested to remain anonymous.

GLOSSARY

Note: Glossary definitions based on those available from the following sources, as well as additional explanations drawn from other sections of this study: Merriam Webster Online, www.merriam-webster.com and Webopedia: Online Computer Dictionary for Computer and Internet Terms and Definitions, www.webopedia.com.

3G: Third generation of mobile communications technology, which allows high-speed internet access through mobile phones

Blog: short for weblog, an online personal journal with reflections, comments, and often links to other websites or blogs provided by the writer; most blogs allow reader comments and are used to foster discussion surrounding certain topics; while most contain reflections on bloggers' personal lives, increasingly they are being used to comment on social and political issues

Blogosphere: all of the blogs on the internet or within a specific country, e.g. the Tunisian blogosphere

Broadband: a high-speed internet connection in which a single wire can carry many channels at once, allowing a high data-transfer rate; necessary for viewing multimedia content

Bulletin Board System (BBS): an electronic message center; most bulletin boards serve specific interest groups; users can post information or products for sale, and other posters can respond

Chat Room: an online location that allows multiple users to engage in a real-time, text-based conversation or discussion

Cybercafe: a commercial location where patrons can use the in-house computers to access the internet for a specified fee and time; most often used by travelers or those without a home internet connection

Cyberspace: the nonphysical world created by computer systems; the internet, for example, creates a cyberspace within which people can communicate with one another, do research, or simply window shop; like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery

DDOS Attack: Distributed Denial of Service Attack; generally consists of the concerted efforts of a person or persons to prevent an internet site or service from functioning efficiently or at all, either temporarily or indefinitely; this is usually done by overloading the attacked website with so many requests for information that it crashes and cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable; those responsible often infiltrate computers around the world and program them to join in the assault as an automated network, or "botnet"

Dial-up: an internet connection over a standard telephone line, usually with a very slow speed that makes it difficult to access some features, especially multimedia applications

DNS: domain name system; an internet service that translates domain names—the appellations commonly used to identify websites, e.g., www.example.com—into numerical IP addresses; because domain names are alphabetic, they are easier to remember, but the internet is actually based on IP addresses; every time a user enters a domain name, a DNS service must translate the name into the corresponding IP address; for example, the domain name www.example.com might translate to 198.105.232.4

DSL and ADSL: digital subscriber line and asymmetrical digital subscriber line; allow data transmission over the wires of a local telephone network, at a faster speed than dial-up permits; the internet connection can be maintained without obstructing telephone use on the same line; ADSL features a greater flow of data in one direction than in the other, so that download speeds are often much faster than upload speeds

Fiber-Optic Cables: Cables made of glass or plastic fibers, used to transmit data. Fiber optic cables have a much greater bandwidth than metal wires typically used for local telephone networks, can carry more data, and are less susceptible to interference

Firewall: a system designed to prevent unauthorized access to or from a private network; can be implemented in both hardware and software; all messages entering or leaving the protected network pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria; while in most countries these are also used by companies to prevent employees from accessing content unrelated to their work, in several countries—most notably China and Iran—firewalls are set up on a national level to prevent citizens from accessing certain content from abroad

Forum: an online discussion group in which participants with common interests can exchange open messages; forums are sometimes called newsgroups

Forum Trolling: the practice of lingering in a chat room or forum and reading the posts instead of contributing to the discussion, often used to denote a "spy" who observes what is being said or discussed and then reports that information to authorities or who attempts to maliciously disrupt conversations or agitate users in a forum or chat room

Hosting Service/Host: a service provider that houses, or hosts, multiple websites on its server computers in exchange for a fee

ICT: information and communications technology, including computers and mobile devices

Instant Messaging/I-Chatting: real-time, text-based communication between individuals in what amounts to a temporary private chat room

IP Address: the numeric address of a computer on the internet; used to identify a computer and network in much the same way as a social security number or national identity number is used to identify a person

ISP: internet-service provider, a company that provides access to the internet for a fee; supplies customers with a software package, a username, a password, and telephone numbers to initiate a connection

IT: information technology, the broad subject concerned with all aspects of managing and processing information

Local Area Network (LAN): A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves

Microblog: A type of blog that allows users to publish short text updates that are disseminated to a large number of followers. Twitter is an example of a microblogging site that allows posts of up to 140 characters

Netizen: citizen of the internet; a person actively involved in the online community

Packet Sniffer: computer software or hardware that can intercept and log traffic passing over a network; often part of a firewall system; can be used to spy on users and collect sensitive information such as passwords

Proxy server: A server, or a computer that sits between a user and a website to intercept requests. Proxy servers have various uses, but in the context of these reports, they typically refer to a tool used to circumvent blocks on accessing certain websites

Real Name Registration: A system by which users who want to post a comment online have to complete a registration form that collects data on the user's real name, ID card number, contact phone or address

Secure Sockets Layer (SSL): a method developed for transmitting private documents and data over the internet; uses two-layer encryption to ensure security; most often used in websites that handle private data, such as credit-card or banking information; denoted by the use of "https" in the URL rather than the standard "http"

SMS/Text Messaging: short-message service; brief text messages of no more than a few hundred characters, sent electronically from one mobile phone to another

Social Networking Site (SNS): a website that enables users to create public profiles and form relationships with the site's other users, e.g., Facebook, MySpace, Orkut

Uniform Resource Locator (URL): the global address of a document or page on the World Wide Web, e.g. http://www.freedomhouse.org/template.cfm?page=383&report=79&group=19 is the URL for *Freedom on the Net*

Universal Serial Bus (USB) Modem: a specific portable USB device that looks similar to a USB flash drive (a data storage device) and can be plugged into any USB port on a computer to allow broadband access to the internet

Value-added Network Service (VANS): a network provider hired to facilitate electronic data interchange or provide other network services; before the arrival of the World Wide Web, some companies formed value-added networks to exchange data with other companies, but contemporary VANS providers focus on offering data translation, encryption, secure e-mail, management reporting, and other services for their customers

Video Sharing: the practice of uploading video clips—including those captured using mobile phones with video features—for viewing by others; some video sharing takes place via paid web-hosting sites, but most occurs on popular free websites such as YouTube

Virtual Private Network (VPN): a way to maintain fast, secure, and reliable

communication by using the internet to connect remote sites or users; often explained as tunneling a smaller network through a larger network, a VPN can be established to circumvent strict internet controls and censorship within a given country; multinational corporations that operate in repressive internet environments often purchase from the government the right to use VPNs to connect to their home offices

VoIP: Voice over Internet Protocol, a category of hardware and software that enables users to make telephone calls via the internet; these calls do not incur a surcharge beyond what the user is paying for internet access, just as users do not pay for sending individual e-mails

Web 2.0: the metaphorical second generation of the World Wide Web; refers to advanced graphical features, multimedia formats, greater interactivity and content production by users, and related online services, including blog hosting, video sharing, and social networking

Wi-Fi: wireless technology that provides an internet or network connection for properly equipped computers, mobile phones, and other such devices within a given physical or geographical area

BOARD OF TRUSTEES

ABOUT FREEDOM HOUSE

Freedom House is an independent private organization supporting the expansion of freedom throughout the world.

Freedom is possible only in democratic political systems in which governments are accountable to their own people, the rule of law prevails, and freedoms of expression, association, and belief are guaranteed. Working directly with courageous men and women around the world to support nonviolent civic initiatives in societies where freedom is threatened, Freedom House functions as a catalyst for change through its unique mix of analysis, advocacy, and action.

- **Analysis:** Freedom House's rigorous research methodology has earned the organization a reputation as the leading source of information on the state of freedom around the globe. Since 1972, Freedom House has published *Freedom in the World*, an annual survey of political rights and civil liberties experienced in every country of the world. The survey is complemented by an annual review of press freedom, an analysis of transitions in the post-communist world, and other publications.
- **Advocacy:** Freedom House seeks to encourage American policymakers, as well as other government and international institutions, to adopt policies that advance human rights and democracy around the world. Freedom House has been instrumental in the founding of the worldwide Community of Democracies, has actively campaigned for a reformed Human Rights Council at the United Nations, and presses the Millennium Challenge Corporation to adhere to high standards of eligibility for recipient countries.
- **Action:** Through exchanges, grants, and technical assistance, Freedom House provides training and support to human rights defenders, civil society organizations, and members of the media in order to strengthen indigenous reform efforts in countries around the globe.

Founded in 1941 by Eleanor Roosevelt, Wendell Willkie, and other Americans concerned with mounting threats to peace and democracy, Freedom House has long been a vigorous proponent of democratic values and a steadfast opponent of dictatorships of the far left and the far right. The organization's diverse Board of Trustees is composed of a bipartisan mix of business and labor leaders, former senior government officials, scholars, and journalists who agree that the promotion of democracy and human rights abroad is vital to America's interests.

1301 Connecticut Avenue, NW, Washington, DC 20036
(202) 296-5101

120 Wall Street, New York, NY 10025
(212) 514-8040