DigitalRightsFoundation
"KNOW YOUR RIGHTS"

A Data Protection Law in Pakistan:
Policy Recommendations by Digital Rights Foundation

Introduction

Data protection is commonly defined *as the law designed to protect your personal information, which is collected, processed and stored by automated means or intended to be part of a filing system*. In other words, it is the *protection of your digital identity*, it enables individuals to determine how they want their information to be used and by whom. Your digital identity takes numerous forms, on the internet or the network, it could be anything corresponding to your physical identity. Data protection laws restrain and shape the activities of companies, governments and other individuals from infringing upon that identity.

Over the last few decades, the rapid and tremendous advancement in communication and information technologies has significantly impacted individuals' ability to protect their digital identity allowing for pervasive collection of personal information, often without the knowledge or consent of the data subjects. In order for individuals to exercise their right to privacy, data protection laws must provide for confidentiality, security and anonymity for their information and communications.

Frank La Rue, the former UN special rapporteur on freedom of expression and opinion, stated that "*Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas*…" expressing his concerns over how even minor privacy incursions could jeopardise political and intellectual culture. He advocated that individuals should be able to communicate anonymously and confidentially in order to express themselves freely. As privacy incursions not only threaten the right to privacy but free expression, association and religious freedom. He confirmed that "*an infringement upon one right can be both the cause and consequence of an infringement upon the other*." Therefore, robust data protection laws must be in place to guarantee the protection of these rights.

Data protection limits what data is collected, for which purpose and how it is collected. For instance, it is possible that mere collection of personal data could threaten privacy. Admittedly, it might be necessary to preserve digital data. Domestic legislation often sets out the period of time that certain categories of document have to be retained for, for potential law enforcement use in the future. For example, *Prevention of Electronic Crimes Act 2016 (PECA)* requires a service provider to retain its specified traffic data for a minimum period of one year or such period as the authority may notify. However, the retention of traffic data for as long as a year is in contravention with the OHCR's report on the interpretation of Article 17 of the ICCPR and is rendered arbitrary and inadequate practice.

Data protection is also intrinsically linked to digital security. The internet travels across national borders but privacy and data protection laws are still based on national sovereignty because the reach of the internet has gone beyond what was originally envisaged. Recent cases of "*cyber war*" attacks are proof of the magnitude of threat to nation states, Stuxnet being the most famous example. Pakistan too, became a victim when its Internet Exchange (PIE)'s was infiltrated by the GCHQ.[1] It seriously undermined the right to privacy of all users of the internet in Pakistan. Therefore, strong data protection mechanisms must be adopted by the State to protect personal data of citizens as well as protect the State from external threats.

Evidently, as the internet penetration and usage grows it increases jurisdictional issues associated with it. Therefore, specific provisions are needed by Pakistan to protect data that enters and leaves the country aiming to facilitate trans-border data flows within the region or between regions and to ensure the continuity of data protection for users.

This would further reap economic and financial benefits of enhanced trade with the European Union member states and similar countries that require their trading partners to have 'adequate' data protection laws. Further, enactment of such laws would provide Pakistan and private organisations operating within with unprecedented trade opportunities. Therefore, the State

[1] Hassan Belal Zaidi, "UK online snooping against Pakistan 'alarming'", *Dawn*, June 24, 2015, https://www.dawn.com/news/1190080.

should take a holistic approach that involves stakeholders in the private sector to foster multi-stakeholder collaboration.

If enacted, data protection laws would further inculcate ethical values of transparency, legitimacy, accountability and concepts of fairness associated with the collection and handling of data in Pakistan. In turn, building trust amongst stakeholders in the State. Additionally, data protection laws would have far reaching benefits for Pakistan's global image by also developing trust amongst foreign investors, businesses and consumers.

Data collection is now typically used as a powerful tool by private organisations seeking to target consumers such as telecom companies selling our data to foreign companies or by governmental institutions using it to profile and surveil civilians under the guise of national security. The recent debate about the legitimacy of Law Enforcement Agencies' (LEAs) collection and scrutiny of university students' personal data is yet another example of arbitrary practice of the State, in the name of national security.

Therefore, our efforts must be focused on two fundamental facets: (1) achieving persistently evolving security/ protection by adopting robust data protection laws with minimum scope for abuse and (2) creating awareness amongst citizens so they are able to exercise their rights.

Is Privacy a fundamental right in Pakistan as per constitution?

The fundamental question whether privacy is a right protected under our Constitution requires an understanding of what privacy means. In the context of Pakistan, *"if privacy is to be construed as a protected constitutional value, it would redefine in significant ways."* Article 14(1) of our Constitution states *"[t]he dignity of man and, subject to law, the privacy of home, shall be inviolable*."

A multitude of democracies including Pakistan and various international treaties exemplify Human Dignity as a fundamental and founding value underlying their constitution or mandate. Human Dignity denotes that every individual – irrespective of caste, creed, colour, religion, gender or material belongings – is entitled to the full measure and protection of law, which guarantees life, liberty, equality and the affording of basic socio-economic amenities necessary for the fulfilment of a purposeful living. The Universal Declaration of Human Rights (1948), in Article 1, also declares, "all human beings are born free and equal in dignity and rights." Nevertheless, despite the agreement on abstract notions of the inviolability of the dignity of humans, disagreement persists over the scope and meaning of dignity, its philosophical foundations, and its capacity to constrain judicial decision-making.

In Pakistan, despite a specific provision of the Constitution, no coherent doctrine of human dignity has emerged in our jurisprudence. Further, the absence of an express constitutional guarantee of privacy still begs the question whether privacy is an element of liberty and an integral part of human dignity, i.e. comprehended within the protection of life as well.

In the Supreme Court of India's recent decision on privacy implications pertaining to the Aadhar card, it was unanimously held that individual privacy is a guaranteed fundamental right. Following the landmark decision, it is time Pakistan realises the significance of upholding privacy rights of its citizens.

Therefore, it is stressed that we must accept the idea of human dignity as a fundamental and overriding concept in our human rights discourse. Now is the time for our honourable courts

to build a narrative in their jurisprudence to interpret article 14 in its true spirit. By interpreting privacy *"in a new and broader light that puts human worth at the centre of the fundamental rights debate"*, allowing for more respect and protection of our privacy.

Nevertheless, there have been precedent-setting cases that suggest that Article 14 can be extended to digital privacy. It was held by the Supreme Court in the landmark Benazir's Case, PLD 1998 SCMR 388 that;
"If a person intrudes into the privacy of any man, pries on the private life, it injures dignity of man and violates privacy of home."

Article 9 further protects the "right to life and liberty" of a person and is often cited when deciding whether an intrusion into the privacy of an individual can affect their quality of life. Taufiq Bajwa vs CDGK (2010 YLR 2165) affirms that the courts interpret Article 9 ("right to life") widely enough to be used to protect the right to privacy.

The Lahore High Court held in M.D.Tahir v. State Bank, 2004 CLC 1680 that the practice of collecting private information of bank holders and presenting them to tax authorities, without any allegation of wrongdoing, was a violation of the right to privacy. The State Bank of Pakistan issued a directive that called for the collection, without any sustainable juridical criteria, all personal information (re: Name, address, NTN Number and NIC Numbers as well amount of money) of individuals who have obtained rupees ten thousand as interest. The directive was struck down on the grounds that "taking of private information without any allegation of wrong doing of ordinary people is an extraordinary invasion of this fundamental right of privacy."

Recently, in Muhammad Munir vs The State, PLD 2017 Peshawar 10, the Defendant was imprisoned and fined for creating a fake Facebook profile using the Plaintiff's name to defame her and then uploaded photos to blackmail her. The court held that it was a breach of her privacy.

Such cases are only the starting point, leading to the right direction. However, the courts have still yet to discover the scope of Article 14 in light of the doctrine of human dignity, as discussed above.

International Obligations

Pakistan ratified the *International Covenant on Civil and Political Rights (ICCPR)* in June 2010. The ICCPR commits Pakistan to ensuring the protection of privacy and other rights that rely on it such as freedom of expression and freedom of association as well as obligates it to take certain legislative measures in order to protect and promote the data privacy and security rights of its citizens.

Article 17 of the ICCPR states that *"no one shall be subject to arbitrary or unlawful interference with his privacy, family or correspondence*."

While the provision explicitly does not use the term "data privacy," the HRC's highly influential General Comment no. 16 clearly assumes that data privacy falls under the scope and meaning of Article 17. It states that "*gathering and holding of personal information on computers, data banks and other devices … must be regulated by law*.

Within the past three decades, a growing number of international bodies have endorsed the HRC's interpretation of the right to privacy as including data privacy. In 2013, the UNGA adopted Resolution 68/167, which was meant to specifically address the growing threats to privacy in the digital age. The Resolution emphasized that "*unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the rights to privacy and to freedom of expression and may contradict the tenets of a democratic society*."

Therefore, Pakistan is obligated to bring its existing data protection laws in line with the Article 17 interpretation and enact "adequate" data protection laws for full compliance. The Drafters of the legislation should fully comprehend the scope of Article 17 in order to be able to draft legislation that identifies the scope of privacy and its limitations.

Existing Legal Regime

The existing legal regime provides no safeguards as there are no proper constitutional and statutory provisions on privacy in Pakistan. Following are just a few provisions of PECA that indirectly and directly regulate data protection.

Prevention of Electronic Crimes Act 2016 (PECA) Contains a number of sections related to data privacy.	**Chapter II of the Act** lists offences and punishments in overly broad language and with fewer safeguards. **Lack of Public Interest Defences** Contrary to S3, individuals would potentially be prosecuted due to a lack of Public Interest defences where unauthorised access to information systems, programmes or data maybe legitimate such as for research purposes or investigative journalism. **S 4 of the Bill criminalises the unauthorised copying or transmission of data.** Whilst the offence includes a requirement of 'intent', as currently drafted, we are concerned that Internet Service Providers could be prosecuted for transmitting data if they are not authorised to do so. It is also noted that the Cybercrime Convention does not include any requirement for States to adopt any provisions of this kind. **S5** poses a similar concern; while there is a requirement for dishonest intention, the provision does not require that such interference result in serious harm.	**Sections 3-5 are** too broad and in breach of the legality requirement under international human rights law. Therefore, they should be revised in line with the requirements of the Cybercrime Convention.

	Legality Requirement All offences associated with unauthorised access lack public interest defences and do not require a legality requirement as should be the case under International Human Rights Law and therefore in contravention of the best practice standards set by the Cybercrime Convention 2001 **No dishonest or malicious intent required** There is no requirement that the offence be committed with the intent of causing harm or by infringing security measures. Therefore, engulfing everyone in, irrespective of their purpose. Thus, failing to recognise that interest groups may legitimately engage in peaceful 'online protest' by seeking to disrupt access to a website without causing any real damage to that site. **S18** effectively **criminalises defamation** in breach of international standards on freedom of expression.	As discussed earlier, in the absence of a legality requirement or an intent requirement, the scope of offences contained in Chapter II is not just limited to criminals but it also extended to all individuals who gain access to unauthorised information. Therefore, all offences listed in Chapter II should be revised to incorporate these requirements. We recommend the decriminalisation of defamation and that criminal law should only be applied in the most serious cases. Similarly, the publication of private information in breach of confidence or the misuse of private information should be

		treated as civil wrongs rather than criminal offences under Chapter II. Moreover, even where defamation is a civil wrong, the law should provide that a statement is not defamatory unless its publication has caused or is likely to cause serious harm to the reputation of the plaintiff. Although attempts at protecting the right to privacy and reputation are legitimate, S18 (2) provides for a new remedy that would allow aggrieved persons to apply for injunctions ordering the removal, destruction or blocking of access to material in breach of section 18 (1). It is stressed that such injunctions are ineffective at achieving their stated purpose due to the nature of the internet itself and therefore should be revised, in light of the concerns raised above.
	S 35 (g) allows an authorised officer has the power to "require any person who is in possession of decryption information of an information system… to grant him access to such decryption information necessary to decrypt data	S 35 (g) should be revised to limit the broad powers granted to any officer authorized by the PTA as they are particularly invasive of the privacy of

	required for the purpose of investigating any such offence.” While the provision provides certain guidance on the way such power should be exercised (acting with proportionality, avoiding disruption, seizing data only as a last resort), the powers vested on the officer are very broad. Their potential for misuse is extremely high. This is particularly so as the power provided could be used to demand the disclosure of encryption keys, thereby exposing individuals at the risk of disclosure of private data beyond what may be necessary to conduct an investigation.	individual's digital communications.

Recommendations

In light of the principles laid out above, we recommend the Government of Pakistan to:

1. Take measures to ensure that state security imperatives do not override the right to privacy in its collection, storage and usage of citizens' data;

2. Ensure that all interception activities comply with the principles of legality, proportionality and necessity, and revise the existing regulation regime at a minimum by bringing it more closely in line with international human rights law;

3. Enact provisions that would inculcate democratic values of transparency, legitimacy accountability and concepts of fairness associated with the collection and handling of data in Pakistan in the private sector by companies, governmental institutions and individuals;

4. Limit the collection of personal information by the government and the private sector and ensure it is obtained by lawful and fair means, only with the knowledge or consent of the individual;

5. Ensure that the information collected is only used for the purpose clearly specified and agreed at the time of collection, and should be accurate, complete and up to date;

6. Take measures to ensure that personal information can only be disclosed, used or retained for the original purposes, except with the knowledge of the individual or under the law, and accordingly it must be deleted when no longer necessary for that purpose;

7. Adopt and enforce reasonable security safeguards to protect personal information from loss, unauthorised access, destruction, use, modification or disclosure;

8. Implement transparency by informing individuals of the collection, purpose, use of their personal information and the organization that is storing it;

9. Enable individuals access and request to amend the information held for the purposes of deletion, rectification, completion or modification;

10. Limit data collection through technological means and careful design, by mathematically restricting further data processing to limit unnecessary access, amongst other privacy measures;

11. Provide clarity by establishing independent accountability mechanisms and reviewing mechanisms of oversight over the surveillance practices of its state agencies to ensure they are subject to independent oversight and guarantee transparency of their mandate and operations in accordance with international human rights standards;

12. Create an Independent Privacy Commission to conduct investigations, act on complaints and impose fines when they discover an organisation or state agency has broken the law;

13. Ensure safeguards to hold data controllers and handlers to account for breach of the above principles and rights. This should include accessing, selling or sharing of personal data for unspecified purposes and without the permission of the data subject;

14. Penalties for misuse of citizens data by government officials, which includes using it beyond the purpose it was originally collected for;

15. Review the *Prevention of Electronic Crimes Act* to ensure conformity with Pakistan's obligations under the ICCPR (Articles 17, 19 and General Comment No. 16);

16. Review all licensing agreements which impose obligations on the private sector to facilitate and/or conduct communication surveillance, and take the necessary measures to ensure that the private sector – in both policy and practice – comply with international

human rights law and standards, in particular in relation to requirements for blanket, indiscriminate data retention;

17. Dismantle legal regimes that require state permission to use encryption or anonymity tools, and ensure its laws, policies, and practices that affect personal use of encryption and online anonymous speech are consistent with its international human rights obligations;

18. Adopt and enforce a comprehensive data protection regime governing any data copied by State authorities to ensure the protection of personal data of it citizens as well as protect the State from external cyber-attacks;

19. Regulate information-sharing with foreign governments and entities by specific laws and subject to independent oversight;

20. Strongly regulate the power vested in any authorized officer of the PTA to obtain decryption of information, subject to clearly defined rules and appeal;

21. Create an independent body to time stamp preservation logs/ documents so it is impossible to create false documents or tamper with data, without it being evident;

22. Ensure data quality of the records held by public bodies by obligating them to keep the data accurate and up to date;

23. Require organizations/ businesses to have public data privacy policies, accessible to users and to require that data storage arrangements have adequate security and restricted access;

24. Draw a clear distinction between unauthorised access of information system or data etc for legitimate purposes such as research or investigative journalism and unlawful access for criminal activity to avoid wrongful criminalisation;

25. Treat the publication of private information in breach of confidence or the misuse of private information as civil wrongs rather than criminal offences under Chapter II of PECA.