

Special Report

How mass surveillance from online advertising puts journalists at risk

August 27, 2026

By Jonathan Rozen

Introduction

Journalist Nicolas Baudoux didn't pay anything to find out where his colleague at L'Echo newspaper in Belgium had been. The locations came free from a data broker based in the U.S.

The broker provided tracking data from mobile devices covering just two weeks of 2025, "but even with that we could identify people" within the sample, which contained about "one million devices and included 100 million locations," Baudoux told CPJ.

German journalist Ingo Dachwitz found details about himself in a similar, free database sample.

"I was very stunned to see some of my data in there," said Dachwitz, who reports for netzpolitik.org and had permitted a weather app to track his location. "As a journalist who has covered these issues for a long time and even knowing an app had been logging my movements, it's very spooky."



Ingo Dachwitz, journaliste pour netzpolitik.org basé à Berlin, a contribué à mettre en lumière les problèmes de confidentialité et de sécurité liés aux courtiers en données et aux systèmes de publicité en ligne. (Photo : Darja Preuss)

These findings came as part of sprawling investigations by several European outlets, offering rare clues into how personal data collected and sold by private companies can be used for targeted surveillance, including of the press.

Journalists are regularly monitored with various forms of surveillance in efforts to intimidate them or expose their sources, often causing psychological trauma. These threats have expanded with the mass surveillance architecture associated with online advertising and the personal data economy, and have been supercharged by artificial intelligence (AI).

“A surveillance apparatus like this is truly unprecedented and it was constructed functionally under everybody’s noses,” Robert Flummerfelt, an investigative journalist and digital safety expert, told CPJ.

Personal data of internet users — including their locations and other intimate details — is being constantly collected and used to inform online advertising strategies in what has grown into a nearly \$1 trillion marketplace. Commonly referred to as surveillance capitalism, this global ecosystem of data extraction, commodification, and use is central to the business model of the world’s biggest tech companies — and is increasingly part of law enforcement tactics and government intelligence operations.

A June 2026 study of laws in Europe and the U.S. found “significant legal gaps and ambiguities” in statutory frameworks “governing the full lifecycle of commercially sourced data.” It also raised concerns over impacts on freedom of the press.

“All of that data can be handed over to states that don’t want to make money off of you. They want to control reporters,” Flummerfelt said. “They want to know who reporters are meeting with, who reporters are talking to, who reporters’ sources are, what they’re working on.”

Research for this report was conducted as part of a Technology and Human Rights Fellowship with the Carr-Ryan Center for Human Rights at the Harvard Kennedy School, which has also published a version of this report.

Read CPJ's guidance for mitigating risks of surveillance from online advertising technology.

The 'surveillance ecosystem'

In a series of interviews, experts told CPJ how journalists are at risk at home and in exile from this architecture of mass surveillance and those that harness it, highlighting several interconnected systems and actors:

- Software development kits (SDKs) and applications that collect data from devices;
- Real-time bidding (RTB) auctions, where users' data is shared;
- Big tech firms facilitating online advertising;
- Data brokers selling individuals' information;
- Advertising intelligence (ADINT) companies offering tools for targeted surveillance; and
- Firms developing spyware delivered via online ads.

Since data is often sold and repurposed after it leaves a device, experts also noted challenges of confirming when journalists may have been targeted via that information in connection with their work. Nevertheless, recognition of such dangers is increasing.

In 2025, France's National Cybersecurity Agency flagged surveillance threats from the online advertising ecosystem and, in late May 2026, U.S. lawmakers wrote to the Pentagon expressing concern over reports that its forces had been targeted using commercially available data.

Top human rights officials are sounding the alarm as well.

“By designing architectures that prioritize data harvesting, private tech actors have created the very infrastructure that States now exploit for surveillance,” Gina Romero, United Nations special rapporteur on freedom of assembly and association, wrote in an April 2026 report.

The same month, Romero and four other UN special rapporteurs jointly warned that “Digital surveillance tools and methods cannot be viewed in isolation but constitute elements of a complex, interconnected and reinforcing surveillance ecosystem.”

“AI systems intensify surveillance threats and activities through their ability to gather and analyse unprecedented volumes of data,” they said.

Channels of collection: SDKs and RTB

Software development kits (SDKs) and real-time bidding (RTB) are two prominent avenues for quietly gathering data on individuals.

SDKs are segments of code that help software developers build applications and can support integration with online advertising systems. Private companies have used SDKs to collect location data that can then be sold to those seeking to follow people.

“[W]e easily traced one Washington Post journalist,” New York Times writers said in a 2019 report examining SDKs and location data from over 12 million phones. “Reporters hoping to evade other forms of surveillance by meeting in person with a source might want to rethink that practice.”

Journalists and researchers have continued to expose how SDKs enable the collection of location data, and tracking systems have become increasingly interconnected.

“Developers [of apps] and advertising SDKs also have a financial incentive to share location data, since it can increase bid prices for an app’s ad space,” Electronic Frontier Foundation technologists Lena Cohen and Bill Budington wrote in an August 2026 report.



Sara Geoghegan, senior counsel at the Electronic Privacy Information Center (EPIC), a Washington, D.C.-based research group. (Photo: Electronic Privacy Information Center)



Arielle Garcia, COO of the digital advertising watchdog organization Check My Ads, emphasized how data extracted through the online advertising ecosystem can be used to track journalists. (Photo: Casual Films)

The RTB system is a marketplace where almost-instantaneous exchanges take place between those offering space for online advertising and others with ads to fill that space. In this exchange, which takes place as someone opens a website or an app that carries ads, a data profile associated with that device and its user(s) is broadcast into the marketplace and various advertisers place bids to show their ads to that user.

“The information that is originally collected and sent into this auction could include...a person’s profile that shows their location, their political affiliations, their employment, which could be sensitive,” Sara Geoghegan, senior counsel at the Electronic Privacy Information Center (EPIC), a Washington, D.C.-based research group, told CPJ. “It can include health information, mental health status. It can include things that a person could be really harmed [by] if that information got out.”

Journalists regularly face attacks on their reputation, which can have a chilling effect on their work.

“Bidstream data harvesting and the SDK data economy ... [are] alive and well today. You do not even need to win an ad auction to be able to harvest data,” Arielle Garcia, COO of the digital advertising watchdog organization Check My Ads, told CPJ in late June 2026. “If you have a particular journalist that you want to go after, you can do that. If you can get them to click on something, you can continue to track them further.”

Advertising IDs, popular apps open doors to personal data, tracking

Profiles sent from phones into RTB auctions do not generally display the name of the associated individual. Rather, each profile is associated with a mobile advertising ID. These IDs, typically assigned by tech and ad companies, are described by Google as “user-resettable identifiers that allow developers and marketers to track activity for advertising purposes,” enabling the matching of data to a “user behind an impression.”

But the U.S. Federal Trade Commission (FTC) has said advertising IDs “provide no anonymity” and AI is making it even easier to associate data with individuals, heightening malicious tracking risks.

“If you are able to verify the mobile advertising ID for a journalist, then you have really quite powerful capabilities,” Wolfie Christl, senior researcher with the University of Toronto-based Citizen Lab research group, who has investigated the consumer data industry for more than a decade, told CPJ.

University of Washington researchers confirmed the ability to track device locations using the RTB system. With knowledge of a target’s advertising ID and regularly used apps, they reliably sent ads to a specific device that would confirm its location when the ad was served.

“You can put the ad associated with the ID and a particular location,” Paul Vines, one of the researchers, told CPJ. “So if that device gets close enough to that point and runs an app where the ad could be shown, then it’ll pop up,” confirming the target’s presence.



Wolfie Christl, Citizen Lab senior researcher and Cracked Labs co-founder based in Vienna.
(Photo: Cracked Labs)

While their study was published in 2017, Vines told CPJ in late 2025 that the advertising industry continued to have “high demand ... for very precise geo-targeting” and the ability to use the system in ways similar to their study hadn’t fundamentally changed.

In 2023, the Irish Council for Civil Liberties (ICCL) reported the risk of foreign state

and non-state actors using RTB to gather data on U.S. and European leadership and military figures.

“It applies to journalists just the same,” Johnny Ryan, one of the reports’ authors, told CPJ, adding “everyone is a target for someone, and their RTB data can be obtained.”

ICCL cited a 2021 marketplace dataset from Xandr, a Microsoft advertising subsidiary, that listed segments of individuals based on specific attributes. Segments identified individuals as “uk_femalejournalists” and “Journalists and News.” Another segment indicated those with interest in the “Committee to Protect Journalists.”

“You can use these kinds of segments for targeting,” said Christl, the second author of the ICCL reports. “You can get a list of people who were sorted into a certain category, like those interested in your organization, or whatever, and then use other data to narrow down individuals for additional tracking or engagement.”



A Microsoft office in New York City in June, 2026. (Photo: Jonathan Rozen)

Xandr was consolidated into Microsoft Advertising in 2025, as the company touted a “new era” of “AI-powered advertising platforms that make personalized advertising simple.”

Replying to questions emailed in June 2026 to Microsoft’s media contact, an account manager with the public relations firm We. Communications said they would provide responses, but did not. As of early August 2026, Microsoft’s privacy statement said users “can opt out of sharing data with third parties for personalized ads.”

In January 2025, ICCL and EPIC filed a complaint with the FTC over Google's RTB system. The complaint alleged the tech giant failed to comply with the Protecting Americans' Data from Foreign Adversaries Act (PADFAA) and Section 5 of the FTC Act, which prohibits unfair or deceptive acts and practices. It cited instances of RTB data being sent to entities in China and Russia.

The FTC did not respond to questions emailed in late June and Geoghegan said in early August 2026 that there had been no substantive updates on the complaint. But the agency has acted in recent years to curb the location data industry.

Questions emailed in June 2026 to Google's press contact received what appeared to be an automated acknowledgment, but nothing further.

Responding to others' coverage of the ICCL reports and the FTC complaint, Google claimed it has the "strictest restrictions in the industry on the types of data we share in real-time bidding" and denied wrongdoing. Earlier this year, following the settlement of a class action case over its sharing user data with hundreds of third parties, Google began offering an option it said would limit information shared via RTB auctions. It is not enabled by default.



A Google office in New York City in June, 2026. (Photo: Jonathan Rozen)

“One of the reasons why this [RTB system] is so harmful is not just that it’s an inherent invasion of privacy to broadcast personal information to many entities that are not regulated and don’t control where that data is going. The next step after this is that other companies purchase this information,” Geoghegan said, describing how companies are able to repurpose data they receive. “Any bad actor or authoritarian regime can purchase information from brokers for relatively cheap.”

404 Media cofounder Joseph Cox, who has reported on these issues for years, agreed that such information could be used to follow journalists and expose who they meet, but noted that purchased data sometimes “isn’t that good” and may need to be “cleaned up” to become useful.

“It’s hard to know exactly how much of a threat it could be to you personally as a journalist,” Cox told CPJ, while emphasizing the importance of precautions like limiting location tracking permissions and being cautious of which applications to download.

In 2025, 404 Media reported the harvesting of location data from RTB associated with popular apps from around the world, including Candy Crush, Tinder, Grindr, Temple Run, My Period Calendar & Tracker, and various news apps. The way the RTB system operates meant that developers of those apps may not have been aware the data was being collected, the report said.

But companies with apps also have financial incentives to take data directly from their users.

“Apps, with their privileged permissions on a device, are able to collect with impunity,” Mike Yeagley, a U.S. military contractor who has helped conduct surveillance using targeted advertising data and has spoken out about its risks, told CPJ. “Every app on your phone has this incentive to monetize the user. They’ve developed the ability to do that. It’s inherent to their business model, and they’re not outsourcing it to third parties.”

Yeagley emphasized that, even as tech companies have offered users options to limit tracking via GPS and advertising IDs (including Apple’s worthwhile options to toggle off permissions), apps continue to gather revealing data, including locations.

“The advertisers...they heard the noise about privacy and they just went deeper into the device,” Yeagley said.

Data brokers and ADINT companies

After going into exile in Berlin, Egyptian journalist Basma Mostafa has been followed and threatened. A commercially available dataset obtained as a free sample and reported in April 2026 by German media showed Mostafa’s “pattern of life,” including her home and other locations she visited. She worried Egyptian authorities may have used such data to track her.



Egyptian journalist Basma Mostafa has been followed and threatened in Berlin, where she lives in exile. She has expressed concern that Egyptian authorities may have used commercially available data to track her. (Screenshot: ISHRGlobal/YouTube)

The Egyptian embassy in Berlin did not respond to CPJ's questions emailed in late June.

“There is a large contagion of data brokers,” Check My Ads Director of Intelligence Iesha White told CPJ, describing a sector of companies that profit from collecting and selling data gathered from “an innocuous looking app” or “your favorite website” carrying online ads.

With so much personal data broadly available through various sources, advertising intelligence (ADINT) companies have emerged offering tailor-made tools to facilitate targeted surveillance.

In 2025, Le Monde journalist Martin Untersinger reported the existence of over a dozen companies harnessing advertising data in this way and offering various services, including tracking of devices in near real time or showing their historical locations, even years into the past.

“The fact that this industry exists adds another layer of danger or another avenue for police forces to get at



Ilesha White, Check My Ads Director of Intelligence, explained how data brokers profit from data extracted from internet users' most basic engagements with popular websites and apps. (Photo: Courtesy of Ilesha White)

journalists,” Untersinger told CPJ. “With advertising intelligence, most of the time the access can be worldwide. So ... any journalist can be targeted.”

Based in the U.S. in Nebraska, Penlink offers a product known as Webloc, which is a “global geolocation surveillance system that monitors hundreds of millions of people based on data purchased from consumer apps and digital advertising,” according to an investigation published in April by Citizen Lab.

Penlink disputed these findings in an email to Citizen Lab, but said Webloc contains location data “tied to device identifiers” and obtains such information “from providers who obtain user consent for location data sharing through SDKs.”

Citizen Lab's research additionally suggested the company may obtain data from RTB sources and found Webloc customers have included Hungarian intelligence, police in El Salvador, and U.S. military and law enforcement agencies. The investigation also found indications that Webloc has been used to track people in Germany, Austria, Italy, Romania, the United Arab Emirates, Israel, Singapore, and Russia.

Reporting on the contracts in their countries, where past surveillance of journalists is well documented, Hungarian reporter Szabolcs Panyi with VSquare and the Salvadoran investigative news site El Faro both noted how Webloc may be used against the press. Webloc's original developer, Cobwebs Technologies, which was acquired by Penlink in 2023, also listed a U.S. journalist as a target in 2020 training materials for a related surveillance product known as Tangles. In its email to Citizen Lab, Penlink described Webloc as a "Tangles module."

Responding to emailed questions, Penlink told CPJ in a July 2026 statement that it had "safeguards to reduce the likelihood that our technologies may be used in ways that are incompatible with applicable legal, regulatory, or ethical frameworks," including "vetting potential customers outside of the U.S. and refusing to work with countries or organizations with a history of disregard for civil liberties."

"Our License Agreement prohibits the use of Penlink products, including Tangles and Webloc, to abuse internationally recognized human rights. Targeting journalists is recognized as a serious violation of human rights under both international humanitarian law (IHL) and international human rights law (IHRL)," Penlink said. It also repeated how Penlink obtained location data from "providers who obtain user consent" for sharing through SDKs and "filter out sensitive locations," but did not directly answer a question about its products' use of RTB data.

Jack Poulson, the journalist who reported the Cobwebs training materials and covers security issues, told CPJ that governments and corporations have various options for tracking members of the press and those they meet.



“I had a source in one of these

Jurre van Bergen, journalist and technical researcher. (Photo: Sofia Celi)

companies, and I won’t say which, that I met up [with] in person,” Poulson recalled. “When that source realized how, if our phones were both in the data set...[the company] could probably figure out we were speaking, they basically had a panic attack and wouldn’t talk to me anymore.”

Experts consistently raised “opacity” as a hallmark of the industry, and a sense that its scale and capacities remain underexposed.

“We don’t know how many companies that do this are out there and leverage ads’ data to track,” Jurre van Bergen, a technologist who worked with Amnesty International’s Security Lab, told CPJ, emphasizing the challenges of confirming cases of targeting. “It doesn’t leave a trace on the phone like spyware would.”

Ad-delivered spyware

Reporting in recent years by Haaretz, Amnesty International, Google's Threat Intelligence Group, and others, indicates the emergence of spyware delivered via online advertising.

In a November 2025 interview, Omer Benjakob, who broke the story with Haaretz, explained the basic steps for delivering spyware through online ads: First, the attacker would de-anonymize the advertising ID associated with the target's device. Then they find that individual in the online advertising marketplace and calibrate their ad to ensure it will be served to that device. And finally they deliver the infected ad to appear when the target opens a browser or app.

"They call it half-click...you have to trigger an ad exposure," Benjakob told CPJ, differentiating the attack process from one-click infections that require clicking a malicious link or zero-click infections that use software vulnerabilities to deliver infections without the target taking any triggering action.

"We use words like 'targeted ads' and I think it's actually quite telling that we use what is actually a military term to describe the way ads are served," Benjakob said. "You're targeted with ads the same way you're targeted by a drone."

Spyware sold by Intellexa, one of the companies reported to be developing this delivery mechanism, can grant near-total access to a targeted device and has been used against journalists. Intellexa's ad-delivered spyware product is known as Aladdin, and Haaretz reported that similar products have been developed by at least two other Israeli firms.

Intellexa founder Tal Dilian did not respond to CPJ's emailed request for comment.

Van Bergen, who helped expose Aladdin, told CPJ that this type of spyware delivery appears to operate through JavaScript code embedded in the targeting advertisement. When the ad opens on the device, a redirection takes place, connecting the device to infrastructure controlled by the spyware operator, and then the infection can be activated.

Benjakob and van Bergen said the emergence of ad-facilitated targeting followed improved security measures from major phone makers like Android and Apple, and rising costs for software vulnerabilities that prompted spyware vendors to look for cheaper options. However, both also noted that confirmed cases of infection from this kind of ad-delivered spyware had yet to be publicly reported.

“The potential for abuse for journalists is huge because we function online as well, and we ourselves see ads as consumers and also function in spaces that are affected by ads,” Benjakob told CPJ, saying that he worried someone could be infected from advertising on one of his stories or any other piece of journalism.

Yeagley told CPJ that he thought the prospect of spyware delivered through an ad impression was “low probability,” but commercially available data could easily be used to understand a target and then trick them into clicking on a link and infecting their device.



Omer Benjakob, reporter with Haaretz. (Photo: Yair Meyuhas)

Risks recognized

“Being tracked through commercial data is not an abstract concern for journalists,” Byron Tau, a Washington, DC-based reporter, wrote in his 2024 book on how access to commercial data has enhanced surveillance powers in the U.S.



Byron Tau, Washington, DC-based reporter. (Photo: Elliott O'Donovan)

“There was an attempt to track a White House reporter who had obtained non-classified but embarrassing information about President Trump during his first term. I don’t know that they did it successfully, but I spoke directly to the person that was asked to do this,” Tau told CPJ. “It is not difficult to imagine that corporate security firms and private investigators are looking for evidence of journalists in this data set and trying to out their sources.”

Separately, CPJ reached the same person and they repeated, on the condition of anonymity, how they were asked to track a U.S.-based journalist — and refused.

“I was like, ‘I’m not fucking touching that request. I don’t care how you frame it as a national security, fucking, presidential. I don’t care. I’m not doing it,’” the person recalled, without disclosing who made the request.

During a hearing in March 2026, U.S. Senator Ron Wyden emphasized the purchasing of Americans location data without a warrant was “particularly dangerous given the use of artificial intelligence to comb through massive amounts of private information,” and called for Congress to pass the Government Surveillance Reform Act.

Another bill before Congress, the Fourth Amendment Is Not For Sale Act, would bar the government from purchasing data, including location and online records, that would otherwise require a warrant to obtain.

“In the age of surveillance capitalism, there exists a marriage of interests between the private sector and states over the expansive collection and analysis of personal data,” wrote Pedro Vaca Villarreal, Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, in a late 2025 report. He also raised concern about companies marketing “a combination of spyware injection and AdInt data.”

‘Inconvenient truth’

Media companies that rely on online ads to make money likely involve themselves and their audiences in RTB exchanges, which netzpolitik.org editor Sebastian Meineck described as an “inconvenient truth” for journalists working to protect their privacy.



Sebastian Meineck, netzpolitik.org editor. (Photo: Philipp Sipos)

“The app of their own media house may be part of the dangerous ecosystem,” Meineck told CPJ. “Media companies are part of the problem as long as they participate.”

While journalists and researchers have also found value in commercially available data for their reporting, Flummerfelt insisted such uses do not justify the ecosystem.

“Mass surveillance endangers everyone, not just journalists, in ways which are so abundant that it’s sort of difficult to overstate,” he said. “What surprising positives emerge indirectly are not a reason to maintain the system.”

Credits

***Jonathan Rozen** is CPJ’s Deputy Director of Research and Analysis. He also serves as a Senior External Advisor with the International Justice Clinic at the University of California, Irvine School of Law and was a 2025-2026 Technology and Human Rights Fellow at the Harvard Kennedy School.*

Featured image: AFP/Andrew Caballero-Reynolds

Editor’s note: The name of researcher Paul Vines has been corrected in paragraph 32, the name of Nicolas Baudoux has been corrected in paragraph 2, and the title of Arielle Garcia has been corrected in paragraph 27 and her photo caption to reflect she is COO, not CEO, of Check My Ads.