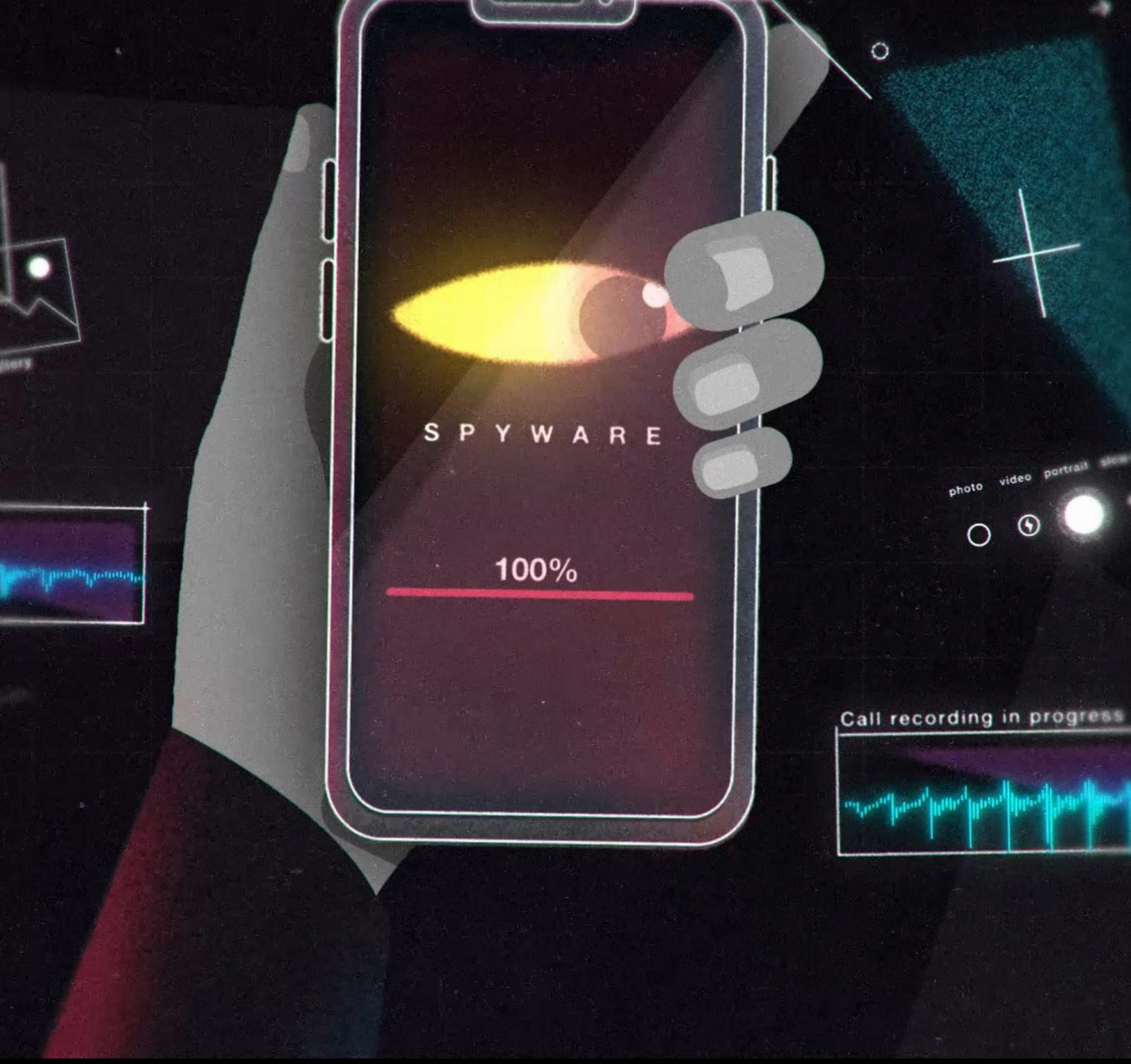


# Zero-click spyware: Enemy of the press

CPJ

A special report by the Committee to Protect Journalists

# Zero-click spyware: Enemy of the press

A special report by the Committee to Protect Journalists

The Committee to Protect Journalists is an independent, nonprofit organization that promotes press freedom worldwide. We defend the right of journalists to report the news safely and without fear of reprisal. In order to preserve our independence, CPJ does not accept any government grants or support of any kind; our work is funded entirely by contributions from individuals, foundations, and corporations.





Design: John Emerson.

Cover illustration by Walid Haddad

# About this report

The development of high-tech "zero-click" spyware – the kind that takes over a phone without a user's knowledge – has emerged as an existential crisis for journalism and the future of global press freedom. The Committee to Protect Journalists conducted numerous interviews with journalists, tech experts, and press freedom advocates around the world about the fear and disruption caused by this insidious software – supposedly only sold for government use against criminals and suspected terrorists. One key finding: that the mere fear of surveillance has had a chilling effect extending far beyond those able to prove infiltration of their phones.

The report also includes CPJ's comprehensive list of policy recommendations for world leaders to combat the arbitrary or unlawful deployment of spyware.

# CONTENTS

# When spyware turns phones into weapons

## How zero-click surveillance threatens reporters, sources, and global press freedom

By Fred Guterl

Aida Alami has always been wary of surveillance. As a journalist from Morocco, a state with a track record of intercepting phone calls and messages of political rivals, activists, and journalists, she habitually took precautions to protect her sources. She avoided using certain keywords and full names in her communications and conducted interviews over Signal, a messaging app that encrypts all content before it leaves a phone. "For some time, we felt really safe on Signal," she told the Committee to Protect Journalists in an interview.

That feeling of safety from using end-to-end encryption evaporated in 2019, when WhatsApp-owner Facebook revealed a vulnerability that allowed hackers to infiltrate smartphones simply by calling someone via the messaging app, without the target having to click on a link. Moroccan authorities had allegedly exploited this now-patched flaw to gain secret access to the phones of journalists and activists, including Aboubakr Jamai, CPJ's International Press Freedom Award winner in 2003.

Like Signal, WhatsApp uses end-to-end encryption to scramble all calls, messages, audio, photo, and video both in transmission as well as on the company's server – an important security feature that prevents governments from intercepting or subpoenaing communications. However, the Facebook disclosure showed that surveillance software could be inserted onto any phone via any app.

That was when Alami realized that just about every precaution she had been taking was now obsolete. "That was really scary," she said.

Since then, Alami has continued to write and report for The New York Times and other publications. But working under the constant threat of surveillance has made her job that much harder. "I know for a fact that a lot of people are scared to talk to me," she said. "A lot of people are scared of writing me, they're scared that my phone is watched. What happens is that you're just paranoid all the time. You assume that your conversations are being read by someone else."

There's nothing new about governments or criminal gangs spying on journalists or activists they fear might expose or discredit them. But the development of high-tech "zero-click" spyware – the kind that takes over a phone without a user's knowledge or interaction – poses an existential crisis for journalism and the future of press freedom around the world.

In interviews with reporters, tech experts, and press freedom advocates in multiple countries, the Committee to Protect Journalists (CPJ) has found that the fear of surveillance extends far beyond those able to prove infiltration of their phones. These attacks – or the mere possibility of them – have already had a chilling effect on sources, who fear their conversations with reporters could expose them to retribution from authorities. Many journalists told CPJ that they are concerned not just for their own personal safety, but for friends and family who may be targeted along with them. Newsroom leaders tell of taking extra security precautions when discussing coverage plans. The awareness that any journalist could be tapped without their knowledge has created profound feelings of powerlessness that could prompt many to leave the profession – or not enter it to begin with. "Violence against journalists is rising," John Scott-Railton, senior researcher

at the University of Toronto's Citizen Lab, told CPJ. "So are digital threats. The damage by tools like Pegasus is contributing to the rise in violence."

Pegasus, a product of the Israeli firm NSO Group, is probably the best-known mobile surveillance program. Like other spyware, it works by insinuating itself into smartphones, but gives the infiltrator particularly free run of the device – access to its microphone and camera, any files or photos stored on the phone, any network connections, contact information, message and browsing histories, passwords, email accounts, recordings and so forth. The purchaser can listen to conversations – even ones that take place over encrypted messaging apps like Signal – all without owners knowing that their phones have been turned into instruments of surveillance.

Perhaps one of the most alarming aspects of the new generation of spyware is that the old methods of defense don't work. Infection can be a zero-click operation; targets needn't open a link or download an attachment. All it takes to pierce the phone's defenses is an unanswered call or an invisible text message. Measures like encryption are only a good protection against a spy who intercepts messages such as texts or emails or voice calls after they've left the phone. When spyware takes possession of a phone, it can eavesdrop on a call before encryption takes place, much like reading a letter over a writer's shoulder before it is sealed in an envelope.

In July 2021, the Pegasus Project found phone numbers of more than 180 journalists on a list of what appear to be potential targets of Pegasus spyware that could turn their mobile phones into listening devices. The NSO Group denies any connection with the Project's list and says that it only sells its product to vetted governments with the goal of preventing crime or terrorism.

Pegasus, however, is just one part of a private surveillance industry now bringing the tools of high-tech spycraft to any nation – or, in theory, any organization or individual – that has the millions needed to pay for the service, experts say. "It's no longer the super states and the super cyber powers, but just about anybody who wants to find out who reporters are talking to, who their sources are, where they're getting their information from," Michael Christie, general manager of global logistics and security at global news agency Reuters, told CPJ.

"Of course, I have much more difficulty meeting and communicating with sources, who are increasingly afraid of the trouble I might bring into their life," Szabolcs Panyi, the investigative reporter, who, along with Direkt36 editor András Pethő, broke the news that Hungary's government had bought Pegasus spyware and was himself a target of the surveillance, said in an interview with CPJ. "Among Hungarian journalists, the biggest fear now is that this [Pegasus] affair will have a chilling effect on sources, and paradoxically this enormous scoop will hinder our work in the long run."

Journalists in multiple countries share similar concerns. For many, spyware infections have been a prelude to harassment and imprisonment under false charges – and sometimes worse. The Guardian reported that around the time Washington Post columnist Jamal Khashoggi was killed and dismembered at Saudi Arabia's Istanbul consulate in October 2018, phones belonging to his close associates and family were targeted with Pegasus spyware. Separately, freelance Mexican journalist Cecilio Pineda Birto was selected for surveillance with the spyware a month before his assassination in 2017, The Guardian reported.

"This is above all an assault on [the] freedom of the press," said Siddharth Varadarajan, founding editor of The Wire, a news website in India, at the International Journalism Festival in Perugia, Italy, in April. "Because when you use Pegasus or…deploy spyware against journalists, you are clearly intending to hamper the work that they do."

## SPYWARE FOR HIRE

Private spyware firms have been on the scene for more than a decade, but these were mainly small operations, Etienne Maynier, a security researcher at Amnesty International, told CPJ. The rise of NSO marked an increase in scale, attracting investors into the spyware market. Last year, NSO was considering an initial public offering.

The publication of the Pegasus Project, an investigative collaboration between Forbidden Stories, Amnesty International, and 17 global media outlets, disrupted those plans. The reporting group acquired a leaked list of 50,000 phone numbers of potential targets of NSO clients. They managed to identify about 1,000 people whose phone numbers were on the list, including 189 journalists. They selected 67 people who they thought were most likely to have been hacked. Amnesty's security lab analyzed the phones and, by July 2021, had found evidence of infections on 23 phones and of attempted penetration on another 14; the count has continued to swell. Among them were heads of state, cabinet ministers, diplomats, military security officers, and journalists from the world's top media


An aerial view of Israeli cyber firm NSO Group at one of its branches in the Arava Desert, southern Israel July 22, 2021. (Reuters/Amir Cohen)

organizations.

After the report came out, the U.S. Commerce Department added NSO to its export-restriction list, blocking hopes of an initial public offering (IPO). (CPJ is part of a coalition of human rights and press freedom groups calling on the U.S. government to keep NSO Group on that list and to hold it responsible for providing Pegasus spyware to governments that have used it for secret surveillance of journalists.) Investors once valued the firm at $1 billion but, according to filings to a London court as reported in the Financial Times in April, came to consider it "valueless." In July, U.S. military contractor L3Harris abandoned its efforts to buy NSO; in August the company's CEO stepped down as part of an internal reorganization.

Still, the spyware industry, which also includes firms like Candiru, Cytrox, and RCS Labs, remains open for business. In June, Google researchers warned victims in Kazakhstan and Italy that they were being targeted by a sophisticated RCS Labs program – known as Hermit – that could go beyond stealing data to recording and making calls. "The emergence of Hermit spyware shows how threat actors – often working as state-sponsored entities – are pivoting to using new surveillance technologies and tactics following the blow-up over repressive regimes' use of Israel-based NSO Group's Pegasus spyware in cyber attacks against dissidents, activists and NGOs, as well as the murders of journalists," wrote cybersecurity news outlet Threatpost.

Zero-click spyware penetrates smartphones by exploiting flaws in the phones' software. The most sought-after is a "zero-day," a term that originally referred to the number of days since a product's release, but which has come to mean any flaw in a device that its manufacturer is not aware of and hence has taken no action to fix. The flaws arise mainly because smartphones are designed to interact easily with the outside world. They are also extremely complex. The latest chips that Apple uses in its iPhones, for instance, have 16 billion physical components (transistors), on top of which are layers of immensely complicated software that govern basic operations of the devices,

coordinate all the apps and cellular network connections and Wi-Fi, and handle a constant flow of data into and out of the phone. Inevitably a new phone hits the marketplace with security vulnerabilities – zero-days – which, for hackers, are like doors left unlocked.

Apple, Google, and other manufacturers of smartphones are constantly on the lookout for zero-days, and they pay hackers for pointing them out. Hackers can make more money, though, by selling zero-days and "exploits" – computer code that takes advantage of the vulnerability to breach the phone's security – to brokers. The highest prices go to "high-risk" vulnerabilities – those that can cause the most damage to the integrity of a phone. Zerodium, a zero-day broker based in Washington, D. C., advertises on its website bounties of up to $2.5 million for "high-risk vulnerabilities with fully functional exploits." Spyware firms like NSO package such exploits for government clients.

## IMPACT ON JOURNALISTS

The growth of the industry appears to have generated a rise in stealth surveillance of opposition leaders, activists, and journalists, as the Pegasus Project and other reports from Amnesty International, Citizen Lab, and other organizations have documented. With infections notoriously difficult to confirm, exact numbers are hard to determine. On the media front, some non-investigative journalists may have been targeted because they'd been in contact with sources already under surveillance. However, the most likely targets are journalists who have written articles that make autocratic governments uncomfortable, such as exposing corruption.

In Morocco, for instance, the Pegasus Project reported that journalist Soulaiman Raissouni was selected for surveillance prior to becoming editor-in-chief of *Akhbar al-Youm*, one of the country's few independent newspapers. He is now serving a five-year prison sentence for sexual assault, which his supporters believe was fabricated. The editor that Raissouni replaced, Taoufik Bouachrine, was also reported to be on the surveillance list. Bouachrine is currently serving a 15-year prison sentence on numerous sexual-offense charges that local journalists and press freedom advocates believe are in retaliation for his critical reporting. Forbidden Stories was unable to obtain access to their phones to confirm the presence of spyware and the Moroccan government has denied ever using Pegasus, but Bouachrine's wife, Asmae Moussaoui, believes she proved her own phone was being monitored after a local tabloid published reports based on false information she'd deliberately used as bait in her calls.

The industry's lack of regulation makes it impossible to prevent abuse of spyware. NSO Group general counsel Chaim Gelfand refused to name specific clients when he addressed the European Parliament's spyware investigative committee in June, but stressed that NSO only sells Pegasus to legitimate governments and said the company had terminated contracts with eight countries in recent years, with some of the cancellations made after the publication of the Pegasus Project. "The system is sold to save lives [but] anything can be misused," he told the parliamentarians.

There is ample evidence to suggest that some who came under surveillance were targeted for political reasons: seemingly because they were opposition politicians or activists or, in the case of journalists, because their work could prove embarrassing to authorities.

In India, for example, the Pegasus Project found traces of the spyware on the phones of two founding editors of The Wire – Siddharth Varadarajan and M.K. Venu – and identified four others writing for the news website as potential targets. The Wire has long been a thorn in the side of the leadership for connecting the ruling Hindu nationalist Bharatiya Janata Party with allegations of corruption, promotion of sectarian violence, and use of technology to target government critics online. Police investigations, criminal defamation suits, doxxing, and threats have dogged the paper's staff, particularly in BJP-led states.

The Indian government denies that it has engaged in unauthorized surveillance, but has not commented directly on a January New York Times report that it acquired Pegasus from Israel in 2017 and has not cooperated with an ongoing inquiry by an expert committee appointed by the country's Supreme Court to investigate illegal use of spyware. In late August, the court revealed that the committee had found malware in five out of the 29 devices it examined, but could not confirm that it was Pegasus.

India's spyware revelations have taken fears of surveillance to new levels. Journalists associated with The Wire told CPJ that the disclosures have made them much more cautious. "We would not talk [about sensitive stories] on the phone," said Ajoy Ashirwad Mahaprashasta, the site's political editor. "Even when we were meeting, we kept our phones in a separate room." Although regular editorial meetings at The Wire are held through Google Meet, sensitive stories are discussed in person.

Swati Chaturvedi, an investigative journalist on the

target list, said her immediate concern following the revelations was protecting her sources. "In Delhi, everyone I know who is in a position of power no longer talks on normal calls," she told CPJ.

Outside the newsroom, the spying revelations have affected journalists' families and friends. "After Pegasus, my friends and family members did not feel safe enough to call me or casually say something about the government," said Arfa Khanum Sherwani, who broadcasts for The Wire on YouTube and is known as a critic of Hindu right-wing politics.

Journalists are equally concerned in other regions around the world. In the Middle East, governments invested heavily in surveillance technology after the Arab Spring protests began over a decade ago. In particular, Israel and the United Arab Emirates have become regional hubs for the nascent spyware industry. At the same time, ruling authorities region-wide passed "cybercrimes" laws, ostensibly for curtailing the spread of misinformation or hate speech. But the laws are vague enough to encompass journalism that officials do not like.

In recent years, several high-profile cases of spyware attacks against international reporters, prominent local journalists, and associates of well-known columnists such as Khashoggi have come to light. Citizen Lab has identified dozens of likely spyware operators throughout the region, particularly in the Gulf, and estimates that the region has some of the highest number of spyware infections in the world. In Jordan, Suhair Jaradat was one of two journalists who were targets of a Pegasus attack by an unknown operator publicized earlier this year. Front Line Defenders, an international human rights group, and

The phone of Jordanian journalist Suhair Jaradat was hacked six times in 2021. (Ahmed Abde/Petra)


L'Indépendant Express director Komlanvi Ketohou is one of the Togolese journalists who may have been selected for spyware surveillance. (Photo: Komlanvi Ketohou)

Citizen Lab analyzed her phone and determined that it had been hacked six times in 2021. Jaradat, whose coverage includes arrests of political opposition figures, told CPJ that she believes whoever initiated the attacks were seeking the identities of her sources; at a cybersecurity conference in February, she learned that her phone had been compromised anew.

The near impossibility of finding smoking-gun evidence that implicates the instigator of an attack is one of the most vexing aspects of hacking in general and mobile spyware in particular. What's left is circumstantial evidence and motives. Authorities in Jordan, for instance, have denied using Pegasus. "In Jordan, authorities stated before that they don't use this spyware, and that people inside the Royal Court were also attacked by it," said Jaradat. "Then who is behind this attack?"

In late 2018, Citizen Lab published a report that also found evidence of Pegasus throughout Africa, including Côte d'Ivoire, Togo, Uganda, Kenya, Rwanda, Zambia, South Africa, and most North African countries. "I spent nightmarish nights thinking about all my phone activities. My private life, my personal problems in the hands of strangers," Togolese journalist Komlanvi Ketohou said after the Pegasus Project reported last year that his phone number was allegedly selected for potential surveillance.

The use of Pegasus on the phones of three reporters from Togo has not been confirmed, but that's done little to ease their fears. Speaking to CPJ 12 months after the Pegasus Project report, they said the prospect of being monitored still generates pervasive paranoia and hinders their communications with sources. "There is a kind of permanent fear," said Ferdinand Ayité, director of Togo's L'Alternative newspaper. "Sources treat us differently. Several people are reluctant to take our phone calls."

In Mexico, one of the world's most dangerous countries for journalists, federal agencies spent more than $61 million on Pegasus alone and up to $300 million on surveillance technology between 2006 and 2018, according to statements by federal Public Safety Secretary Rosa Icela Rodríguez in 2021. New disclosures emerged in October

2022, when a joint investigation by three Mexico-based rights groups and Citizen Lab found evidence of Pegasus infections on the devices of two Mexican journalists and a human rights defender between 2019 and 2021 – infiltration that occurred after Mexican President Andrés Manuel López Obrador's 2018 promise to end illegal surveillance. López Obrador denied on October 4 that his administration had used Pegasus to spy on journalists and activists. The previous Mexican administration also denied using the technology on high-profile journalists, including investigative reporter Carmen Aristegui and several people close to her, as well as Griselda Triana, the widow of journalist Javier Valdéz, who was murdered in Sinaloa in May 2017, and two journalists of RíoDoce, the magazine he co-founded.

In Latin America, the International Network of Journalists found that almost every country has purchased or expressed interest in licenses for surveillance technology over the last decade. A trove of leaked documents published by Wikileaks in 2015 and summarized in a 2016 report from Chile-based digital rights organization Derechos Digitales found that 13 countries in the region bought licenses from or contacted Hacking Team, a now defunct Italian company that sold surveillance malware to public officials around the world. In January 2022, an investigation by Access Now, a global digital rights organization, and Citizen Lab, in collaboration with Front Line Defenders and other organizations, confirmed 35 cases of journalists and members of civil society in El Salvador whose phones were infected with Pegasus spyware between July 2020 and November 2021. The hacking took place while the journalists and outlets were reporting on sensitive political issues involving the administration of President Nayib Bukele, according to the report.

"Surveillance technology is so dangerous in Latin America because of the absolute lack of transparency," Gaspar Pisanu, Access Now's Latin America policy and advocacy manager, told CPJ in an interview. "There's no way of knowing what technology is being used, or how. We don't know any statistics, what kind of data is being accessed, who is in charge of these programs, what type of contracts they have. Regardless of whether it's a democratic or authoritarian government, we're not able to know."

While headlines tend to focus on illegal surveillance and the use of spyware to target high-profile individuals, sources told CPJ that the gray area between what's legal and what's not leaves ample space for abuse by authorities. "Laws on access to information have very broad exceptions for national security concerns," which allows officials to justify surveillance with relatively little oversight, said Veridiana Alimonti, associate director for Latin America policy at the U.S. digital rights group Electronic Frontier Foundation.

"Even the possibility that these tools may be used affects journalists, media outlets, the entire community," said Ángela Alarcón, Access Now's campaigner for Latin America and the Caribbean. "Journalists are going to engage in self-censorship, they have to invest in other means of communicating, safer tools and channels, mental health support. It impacts the work of journalists, their finances, their motivation."

In Hungary, journalists told CPJ that meetings with sources have gotten slower and more complicated to arrange. Sources are more reluctant to meet. Interviews often take place outdoors with cell phones left behind. Panyi, the investigative journalist for Hungarian outlet Direkt36, found out from Amnesty International that he'd been hacked with Pegasus for six months. He subsequently investigated the hacking of other high-profile media targets, including Zoltán Varga, investor and owner of the country's biggest independent news site, 24.hu.

The surveillance of Varga started during a dinner party – "just a friendly gathering," he told CPJ – at his house in Budapest in June 2018, shortly after Viktor Orbán won a third consecutive term as prime minister. All seven people at the dinner were selected for possible surveillance, and at least one had traces of Pegasus on their phone, according to a forensic analysis. "Using this kind of technology in such a situation for me just shows how much the government is afraid of its opponents," Varga told CPJ.

Privately sold spyware is not the only tool government authorities use for high-tech digital spying, of course. Little has been reported, for example, about any widespread use of targeted spyware in countries like China and Myanmar, identified as the world's top two jailers of journalists in CPJ's 2021 prison census.

China has home-grown surveillance methods for tracking its citizens in general and specific groups like reporters in particular. In late 2019, Chinese authorities began requiring journalists wanting to obtain press cards to download an app called "Study the Great Nation," which effectively doubles as spyware. According to the Washington Post, Radio Free Asia's initiative Open Technology Fund found that the Android version of the app "collects and sends detailed log reports on a daily

Journalists and activists protest outside the Attorney General's Office in Mexico City after a 2017 report that their smartphones had been infected with spyware. (Reuters/Carlos Jasso)

basis, containing a wealth of user data and app activity." In June, a New York Times investigation found that Chinese authorities collected more personal data about its citizens than was previously known. "Phone-tracking devices are now everywhere," said the report. "The police are creating some of the largest DNA databases in the world. And the authorities are building upon facial recognition technology to collect voice prints from the general public."

In Myanmar, CPJ has been unable to confirm if spyware was used to obtain information about the scores of journalists who have been arrested and detained since the February 2021 military coup or if it came from forensic data extracted from phones at checkpoints. Local journalists, however, remain hyper-aware of the threat that military authorities still have access to the surveillance technologies bought by the previous civilian-military government.

"Ever since the coup, we journalists are on high alert and vigilant about being spied upon by the authorities given the country's history with the notorious military intelligence unit," said Dominic Oo, the pseudonym under which a local Yangon-based freelance reporter contributes to both local and foreign publications because he fears military reprisals. "Long gone are the days where I am able to walk around town and interview people or just call up a contact on my phone, as this would risk both the interviewer and the interviewees," Oo told CPJ. "It's a dystopian nightmare for local journalists reporting the truth about the junta's brutality."

Nyan Linn Htet, editor of the independent Mekong News Agency, told CPJ via messaging app that journalists were aware of reports that Myanmar's military is using spyware and other forms of surveillance to monitor calls by journalists and activists. "We feel totally unsafe using direct phone calls and have had to change our behavior in gathering the news," said Nyan Linn Htet. "The impact is that it makes it difficult to gather news, data and information, particularly in verifying reports because most people

in rural areas are not familiar with encrypted messaging apps."

## FIGHTING AN INVISIBLE ENEMY

Since spyware can be so stealthy, it's impossible to know for how many journalists have been hacked.

Getting a definitive example of spyware that is installed in a phone is "exceedingly rare," said Steven Adair, CEO of Volexity, a cyber security firm that performs forensics for The Associated Press, in an interview with CPJ. "There isn't a really good way to track a lot of the malware, and there's not really a good way to inspect phones. By and large, no one can actually tell you, 'Hey my phone got compromised.' Because there isn't really any [diagnostic test] you can run that will tell you your phone has been exploited."

Citizen Lab's Scott-Railton did a back-of-the-envelope calculation based on an investigation of WhatsApp infections in 2019. During two weeks of observation, Citizen Lab found that 1,400 Android users had been infected with Pegasus (though not all were zero-click infections). Assuming infections occurred in iPhones at the same rate, that comes to 2800 infections in two weeks, a rate of 75,000 infections a year. "And that's just for Pegasus," he said. "It's never been a less safe time to be a journalist."

Security experts at news organizations Reuters and The Associated Press, who between them employ several thousand journalists around the world, say that while they consider spyware a huge potential threat, they haven't yet seen much of it in practice. "We have 4,000 journalists working for us, divided between staff and freelancers," said Reuters' Christie. "That said, when it comes to malware and Pegasus and the like it's very hard to quantify the threat."

That uncertainty may be the most pernicious aspect of spyware. In the long-term, journalists who feel threatened by an invisible enemy that could expose their sources and their private lives to public scrutiny may start to shy away from controversial investigations, curtailing their publications' coverage, and dealing a blow to press freedom.

"All the previous incidents of phone tapping seemed like an innocent act compared to this," The Wire's Venu told CPJ. "Earlier it was just one conversation they would tap into. They wouldn't see what you would be doing in your bedroom or bathroom." Now, fear of being bugged may lead to "self-censorship," he said. "When someone gets attacked badly, that journalist can start playing safe."

Several factors conspire to make spyware difficult to find on phones. The phones themselves are designed to be hard to break into, which makes them impervious to low-level nuisance malware but also, ironically, makes it more difficult to devise anti-spyware protection. Pegasus-like hacks also generally happen silently, though on occasion targets report their phones operating "hot" or having shorter-than-usual battery life. And since spyware is likely to be erased when a phone is updated or reset, it's difficult for security experts to study.

Amnesty's forensics team had to work mightily to overcome these limitations during the Pegasus Project investigations. Their evidence did not include Pegasus code nor any observation of the actual program in action. Rather, the team used several indirect indicators that Pegasus had once been active on the phones. They made use of an iPhone feature that tracks certain kinds of activity on the phone's operating system to flag "suspicious processes" consistent with Pegasus infection. They found records of website addresses (URLs) that Pegasus software has been known to use. And they found other suspicious behavior related to Apple's iMessage, iMusic, and Facetime apps, which had known vulnerabilities.

"What we found is that the backups of iPhones and several other logs have some data that keep traces of Pegasus," Maynier told CPJ. "Since NSO moved in 2018 to zero-click attacks, [forensics] has been more challenging."

Protecting against spyware is equally challenging. Absent solid information on how many infections journalists have acquired, Reuters and AP have focused on making sure they're taking whatever security precautions they can and emphasizing the need to educate journalists on the risks. AP advises its reporters to keep separate phones for work and personal use. It also installs "mobile device management" software on reporters' work phones, which allows the security staff to monitor the phones for suspicious activity. "In terms of tracking Pegasus, we're not doing anything in that area right now," said Ankur Ahluwalia, a member of AP's security team. "The tool sets available to do that remotely are very limited." CPJ's digital safety team recommends that journalists always take measures like updating their operating systems, apps, and browsers, and that high-risk targets consider having several phones that they cycle through – perhaps changing their phone every week or buying low-cost burner phones every few months.

Harlo Holmes, chief information security officer and director of digital security at the U.S. nonprofit Freedom


Citizen Lab's John Scott-Railton, shown here testifying before a Polish Senate commission in Warsaw in January 2022, told CPJ that tools like Pegasus are contributing to the rise in violence against journalists. (AP/Czarek Sokolowski)

of the Press Foundation, cautions against giving in to a feeling of helplessness. "I see a lot of what I call security nihilism, in that they'll say, 'Nope. It doesn't matter. I had a password manager, I had two-factor authentication. I did all of these things to protect myself. And guess what, everybody still got Pegasus.' As an advocate for digital security in newsrooms, that's something I really do worry about." Holmes advocates "compartmentalization" – using different phones for work and personal lives. "Newsroom managers and editors, and anybody who has control over a budget, should be mindful of this."

## LIMITED OPTIONS

The difficulty of individuals being able to defend themselves against spyware makes it clear that governments and global institutions have to step in. Surveillance technology – and the demand for it – is unlikely to disappear. The challenge now is for governments and rights advocates to find ways to regulate the industry and prevent their products being used as a tool to abuse freedom of speech and other rights.

David Kaye, a law professor at the University of California Irvine and a former United Nations special rapporteur for freedom of opinion and expression, believes that it's time for governments to ban spyware for its violation of international human rights law. "No government should have such a tool, and no private company should be able to sell such a tool to governments or others," he writes in a column for CPJ.

Other potential measures suggested to curb the use of spyware include:

A moratorium on the sale, use, and transfer of surveillance tools pending implementation of regulations that respect human rights – as called for by more than 180 civil society organizations and independent experts, including CPJ.

Restrictions on imports and exports: The U.S. has imposed import restrictions on NSO Group and pressure is growing in the European Union to implement a

regulation (EU law) on the export of dual-use surveillance technology by EU-based companies. The legislation seeks to prevent exports from leading to human rights harm in countries where journalists are targeted and under surveillance because of their work.

An internationally regulated treaty allowing sales only to signatory governments that pledge to obey the rules of spyware use – a version of the "non-proliferation agreement" suggested by NSO Group's vice president for compliance, Chaim Gelfand, at a June hearing of the European Parliament.

Holding spyware manufacturers legally accountable for illicit surveillance using their programs, as in lawsuits filed by Apple and WhatsApp-owner Facebook against the NSO Group after Pegasus infiltrated users' phones through the tech companies' devices and platforms.

However, this patchwork of responses leaves those targeted for surveillance with limited options for finding accountability or justice.

One reason is that spyware has proliferated at such a speed that many governments do not have the legal and regulatory structures in place to hold violators accountable. Another is that it's seldom possible for victims even to prove who is spying on them without cooperation from the spyware companies, which invariably refuse to identify their clients on the basis of non-disclosure agreements and national security claims.

Victims and civil society seeking investigations are also often dependent on governments to transparently investigate themselves. If the intrusion takes place beyond national borders, prosecuting or seeking civil remedies can be difficult, especially if the offending state is authoritarian or has a history of evading accountability.

Even in democratic societies, the political will to restrict spyware may be lacking. A New York Times investigation notes that Pegasus helped Mexican authorities capture Joaquín Guzmán Loera, the drug lord known as El Chapo, and that European investigators have used the program to uncover terrorist plots and combat organized crime. Governments are reluctant to lose this surveillance capability for themselves, and many citizens may be willing to sacrifice their private information in the name of protecting national security.

The challenge now is whether legislators and rights advocates can craft an effective global combination of laws, regulations, awareness, and technological solutions to prevent abuse of surveillance technology – and whether they can do it before journalists' ability to do their jobs is irreparably damaged by the threats to their safety and sources. ◆

*Fred Guterl is an award-winning journalist and editor who has covered science and technology for more than 30 years. Currently special projects editor for Newsweek, he is a former executive editor of Scientific American and the author of "The Fate of the Species: Why the Human Race May Cause Its Own Extinction and How We Can Stop It."*

*With additional reporting by Jan-Albert Hootsen in Mexico City, Kunal Majumder in New Delhi, Attila Mong in Berlin, Alicia Ceccanese in Washington D.C., Shawn Crispin in Bangkok, Tom Gibson in Brussels, Iris Hsu in Taipei, Muthoki Mumo in Nairobi, Jonathan Rozen in New York, Justin Shilad in New York and Natalie Southwick in New York.*

# Hungarian journalists targeted by spyware have little hope EU can help

By Attila Mong

Szabolcs Panyi was not even remotely surprised when Amnesty International's tech team confirmed in 2021 that his cell phone had been infiltrated by Pegasus spyware for much of 2019. Panyi, a journalist covering national security, high-level diplomacy, and corruption for Hungarian investigative outlet Direkt36, had already long factored into his everyday work that his communications with sources could be spied on. "I was feeling a mix of indignation, humiliation, pride and relief," he told CPJ of his response to the Amnesty news.

The indignation and humiliation were from seeing himself and other prominent journalists included on a list of convicted criminals and known mob figures considered to be threats to Hungary's national security. The pride was because the Hungarian government, which routinely ignored his reporting questions, thought it was worth spending tens, if not hundreds, of thousands of dollars on his surveillance; the relief was the validation that his earlier suspicions about being spied on were not a sign of paranoia.

Other Hungarian journalists targeted for surveillance expressed similarly ambiguous emotions in interviews with CPJ. And all were skeptical that any future recommendations by the European Parliament's committee of inquiry into Pegasus and other spyware, expected next year, would bring much relief in a country where independent media face an increasingly hostile press freedom climate under the government of right-wing Prime Minister Viktor Orbán.

Panyi, who continues to relentlessly investigate the surveillance scandal, is one of the few journalists still giving regular interviews to Hungarian and international media about his surveillance. Three other CPJ interviewees said that while they were making an exception in talking to the organization, they'd otherwise stopped making public statements on their experience because they did not want their Pegasus targeting to define their lives.

The three – crime reporter Brigitta Csikász, Zoltán Varga, owner of one of the country's biggest independent news sites, 24.hu, and a reporter who asked not to be identified for fear that further publicity would negatively

Direkt36 journalist Szabolcs Panyi (Photo: Mira Marjanovic)

Hungary's Prime Minister Viktor Orbán arrives at the Informal EU 27 Summit and Meeting within the European Political Community in Prague on October 6, 2022. Independent media have faced an increasingly hostile press freedom climate under his government. (Reuters/David W Cerny)

impact his career – were named as targets in July 2021, when Panyi, who, along with Direkt36 editor András Pethő, broke the story for Direkt36 as part of its reporting for the Pegasus Project, an international investigation that found the phone numbers of more than 180 journalists on a global list of potential spyware targets. (The NSO Group, which makes Pegasus, denies any connection with the Project's list and says that it only sells its product to vetted governments with the goal of preventing crime or terrorism.)

Along with Panyi, all the journalists recounted signs that they were under physical and digital surveillance before they were aware of Pegasus being used against them, and all said that their private and professional lives had changed since the scandal broke last year.

Csikász, who covers corruption, told CPJ in a phone interview that she had seen numerous signs that people might be watching her and was warned by friends for years that her phone might be monitored. "I did not get a heart attack, I was not at all traumatized," she told CPJ in a phone interview about her reaction to the news that Pegasus was used to monitor the contents of her phone between early April and mid-November 2019.

Csikász has even managed to find some humor in her situation. "My friends took it real easy, most of them just crack jokes and my family took it as a sign of prestige and importance. For them, it is as if I was awarded with a special journalism prize," she said. She added that the publicity surrounding the disclosures had even prompted some sources to contact her because they heard about her in the news. "I was not, and I have not, become paranoid," she told CPJ.

Still, Csikász, who currently works for daily tabloid newspaper Blikk and was reporting for the investigative outlet Átlátszó, remains concerned about the intrusion. "As a journalist, I respect my country's laws and my profession's ethical standards and I consider the possibility of being spied on as part of my job," she said. However, she


'We say no to your observation!' Participants walk in front of a poster showing Hungary's Prime Minister Viktor Orbán during a July 26, 2021, protest in Budapest against the Hungarian government's use of Pegasus spyware to monitor journalists, opposition leaders and activists. (Reuters/Marton Monus)

would like to know which of her numerous investigations were considered threats to national security.

Varga told CPJ in a video interview that he'd attracted government attention when he started investing in media in 2014. This scrutiny increased, especially when he made it clear around 2017 that he would not be willing to sell his assets in spite of quiet threats and warnings from businesspeople linked to the government. In recent years, he said, he had spotted people sitting in cars parked outside his house and apparent eavesdroppers sitting next to his table at restaurants. He recalled that his phone calls were often interrupted, he once heard a recording of a call played back from the start, and at one point German tech experts provided proof that his android phone had been hacked.

The Direkt36 investigation found Varga's Pegasus surveillance started around the time he invited six people to a dinner in his house in Budapest in June 2018, two months after Orbán won a third consecutive term as prime minister. All seven participants of the dinner were selected as potential candidates for surveillance and at least one of their phones showed evidence of infection under Amnesty's forensic analysis.

"I was only surprised that the regime used this type of high-level technology to spy on an otherwise innocent gathering of intellectuals," Varga told CPJ in a video call. "It was far from being a coup, it was just a friendly gathering. We discussed the very high level of corruption in Hungary's ruling elite and how to find ways to expose it. Using this kind of technology in such a situation for me just shows how much the government is afraid of its opponents," he said.

The reporter who spoke on condition of anonymity was also surprised that the government would deploy such high-tech spyware against journalists. Although he'd seen indications of occasional physical surveillance, the Pegasus infiltration "came out of the blue and was a real shock to me," he said in a phone interview. His "dark period" only eased when the fact of his surveillance was publicly reported. "Since then, I prefer not to speak about it and share my experiences with anyone but my friends," he told CPJ.

Panyi said that the way he communicates with sources has now become much slower and more complicated. "Of

course, I have much more difficulty meeting and communicating with sources, who are increasingly afraid of the trouble I might bring into their life," he told CPJ in a phone interview. He uses various secure digital tools and applications, is mindful about what networks he connects to on his computer or mobile phone, regularly goes to meetings without his phone, and continues to take physical notes.

Varga says the spyware disclosures have harmed some of his business ventures. "The Pegasus scandal made it obvious for both my business and private contacts that it might be risky to talk to me and they might also get exposed, which people obviously try to avoid," Varga told CPJ, adding that acquaintances now crack Pegasus "jokes" in most of his meetings. "As a result of this whole affair, I have much less phone calls, more walking meetings outside, without phones in the pocket," he said.

Many companies, including advertising agencies and advertisers for his news site, seem to prefer to avoid doing business with him, and their loss is not offset by the small number of ad-buyers who now see the site as an important media voice, said Varga. "I have become kind of toxic for my environment," he told CPJ.

The reporter who preferred not to be named said that his phone now "stays outside" whenever he sees friends and family and he uses a special anti-tracking case when he attends professional meetings.

Hungary's government acknowledged in November 2021 that it had bought Pegasus spyware, but says that its surveillance of journalists and political critics was carried out in accordance with Hungarian law.

A government spokesman said that journalists might have been monitored because some of their sources were under surveillance on suspicion of crimes or terrorist links, not because the journalists were the direct targets of the investigations.

In January, the Hungarian National Authority for Data Protection and Freedom of Information issued a 55-page report, which concluded that in all the cases they investigated, including those involving journalists, all legal criteria for the application of the spyware were met and the spyware was used to protect Hungary's national interests.

These responses have left the journalists who spoke to CPJ with little hope that anyone will be held accountable for the intrusion on their lives. Nor do they expect help from the institutions of the European Union, where officials themselves have been targeted by spyware as they grapple with mounting political pressure over how to hold member states accountable for any breaches of the rule of law.

As the European Parliament's committee of inquiry looks at the mountain of evidence that surveillance spyware has been used in EU countries and against EU citizens, the EU Commission lacks the powers to hold member states to account, and has been forced to refer those seeking justice to their national courts.

Surveilled journalists might eventually get EU relief if a new draft European Media Freedom Act, released on September 16, becomes law. The Act could give journalists a path to file a complaint to the EU's Court of Justice if they or those close to them are subject to the unjustified use of spyware. However, the Act still has to be reviewed by EU institutions and member states and may not survive in its current form.

Meanwhile, Panyi does not believe Hungary's courts can provide any relief. "The laws regulating national security, including surveillance, are so broadly formulated that it is legal to wiretap and surveil anyone," he told CPJ. Noting that there was no independent oversight of the surveillance process, he added that "legal" in these cases meant only that "everything has been properly documented, and the necessary stamps are where they should be."

In June, Panyi saw his concerns confirmed when the Central Investigation Prosecutor's Office announced it had terminated its own investigation into the allegations of illegal surveillance of journalists and opposition politicians, citing absence of a crime. "A broad investigation which included classified documents found no unauthorized and secretive collection of information or the unauthorized use of a concealed device," said the investigators.♦

*Additional reporting by Tom Gibson in Brussels*

*Attila Mong is a freelance journalist and CPJ's Berlin based Europe representative. He is a former John S. Knight Journalism Fellow and a Hoover Institution research fel low, both at Stanford University. He was awarded the Pulitzer Memorial Prize for Best Investigative Journalism in 2004 and the Soma Investigative Journalism Prize in 2003.*

# In India's hardest-hit newsroom, surveilled reporters fear for their families and future journalists

By Kunal Majumder

M.K. Venu, a founding editor at India's independent non-profit news site The Wire, says he has become used to having his phone tapped in the course of his career. But that didn't diminish his shock last year when he learned that he, along with at least five others from The Wire, were among those listed as possible targets of surveillance by Pegasus, an intrusive form of spyware that enables the user to access all the content on a target's phone and to secretly record calls and film using the device's camera.

"Earlier it was just one conversation they [authorities] would tap into," Venu told CPJ in a phone interview. "They wouldn't see what you would be doing in your bedroom or bathroom. The scale was stunning."

The Indian journalists were among scores around the world who learned from the Pegasus Project in July 2021 that they, along with human rights activists, lawyers, and politicians, had been targeted for possible surveillance by Pegasus, the spyware made by Israel's NSO Group. (The company denies any connection with the Project's list and says that it only sells its product to vetted governments with the goal of preventing crime or terrorism.)

The Pegasus Project found that the phones of two founding editors of The Wire – Venu and Siddharth Vardarajan – were confirmed by forensic analysis to have been infected with Pegasus. Four other journalists associated with the outlet – diplomatic editor Devirupa Mitra, and contributors Rohini Singh, Prem Shankar Jha, and Swati Chaturvedi – were listed as potential targets.

The Indian government denies that it has engaged in unauthorized surveillance, but has not commented directly on a January New York Times report that Prime Minister Narendra Modi agreed to buy Pegasus during a 2017 visit to Israel. The Indian government has not cooperated with an ongoing inquiry by an expert committee appointed by the country's Supreme Court to investigate illegal use of spyware. In late August, the court revealed that the committee had found malware in five out of the 29 devices it examined, but could not confirm that it was Pegasus.

However, Indian journalists interviewed by CPJ had no doubt that it was the government behind any efforts to spy on them. "This government is obsessed with journalists who are not adhering to their cheerleading," investigative reporter Chaturvedi told CPJ via messaging app. "My journalism has never been personal against anyone. I don't understand why it is so personal to this government." For Chaturvedi, the spying was an invasion of privacy "so heinous that how do you put it in words."

Overall, the Pegasus Project found that at least 40 journalists were among the 174 Indians named as potential targets of surveillance. With six associated with The Wire, the outlet was the country's most targeted newsroom. The Wire has long been a thorn in the side of the ruling Bharatiya Janata Party (BJP) for its reporting on allegations of corruption by party officials, the party's alleged promotion of sectarian violence, and its alleged use of technology to target government critics online. As a result, various BJP-led state governments, BJP officials, and their affiliates have targeted the website's journalists with police investigations, defamation suits, online doxxing, and threats.

Indian home ministry and BJP spokespeople have not responded to CPJ's email and text messages requesting

Supporters of the Bharatiya Janata Party (BJP) hold a giant cutout of India's Prime Minister Narendra Modi at a public meeting in Secunderabad on July 3, 2022. Modi's government denies using spyware to surveil journalists but has not cooperated with a Supreme Court investigation. (AFP/Noah Seelam)

comment. However after the last Supreme Court hearing, party spokesperson Gaurav Bhatia criticized the opposition for "trying to create an atmosphere of fear" in India. "They [Congress party] were trying to spread propaganda that citizens' privacy has been invaded. The Supreme Court has made it clear that no conclusive evidence has been found to show the presence of Pegasus spyware in the 29 phones scanned," he said.

As in so many other newsrooms around the world, the Pegasus Project revelations have prompted The Wire to introduce stricter security protocols, including the use of encrypted software, to protect its journalists as well as its sources.

Ajoy Ashirwad Mahaprashasta, political editor at The Wire, told CPJ in a phone interview that as part of the new procedures, "we would not talk [about sensitive stories] on the phone." While working on the Pegasus project, the Wire newsroom was extra careful. "When we were meeting, we kept our phones in a separate room. We were also not using our general [office] computers," he said.

Venu told CPJ that while regular editorial meetings at The Wire are held via video call, sensitive stories are discussed in person. "We take usual precautions like occasional reboot, keep phones away when we meet anyone. What else can we do?" he asks.

Chaturvedi told CPJ via messaging app that she quickly started using a new phone when she learned from local intelligence sources that she might have been under surveillance. As an investigative journalist, her immediate concern following the Pegasus Project disclosures was to avoid compromising her sources. "In Delhi, everyone I know who is in a position of power no longer talks on normal calls," she said. "The paranoia is not just us who have been targeted with Pegasus."

"Since the last five years, any important source I'm trying to talk to as a journalist will not speak to me on a normal regular call," said Arfa Khanum Sherwani, who anchors a popular political show for The Wire and is known as a critic of Hindu right-wing politics. Sherwani told CPJ that her politician sources were the first ones who moved to communicate with her on encrypted messaging platforms even before the revelations as they "understood that

something like this was at play."

Rohini Singh similarly told CPJ that she doesn't have any conversations related to her stories over the phone and leaves it behind when she meets people out reporting. "It is not about protecting myself. Ultimately it is going to be my story and my byline would be on it. I'm essentially protecting people who might be giving me information," she said.

Journalists also say they are concerned about the safety of their family members.

"After Pegasus, even though my name per se was not part of the whole thing, my friends and family members did not feel safe enough to call me or casually say something about the government. Because they feel that they are also being audiographed and videographed [filmed or recorded]," said Sherwani.

Chaturvedi told CPJ that her family has been "terrified" since the revelations. "Both my parents were in the government service. They can't believe that this is the same country," she said.

Venu and Sherwani both expressed concerns about how the atmosphere of fear could affect coverage by less-experienced journalists starting out in their careers. "The simple pleasure of doing journalism got affected. This may lead to self-censorship. When someone gets attacked badly, that journalist can start playing safe," said Venu.

Said Sherwani: "For someone like me with a more established identity and career, I would be able to get people [to talk to me], but for younger journalists it will be much more difficult to contact politicians and speak to them. Whatever they say has to be on record, so you will see less and less source-based stories."

Ashirwad agreed. "I'm very critical of this government, which is known. My stand now is I shall not say anything in private which I'm not comfortable saying in public," he said. ◆

*CPJ's India representative Kunal Majumder has worked for outlets including the Indian Express, Rajasthan Patrika, Tehelka and Vice. He is a winner of the Statesman Award for Rural Reporting and UNDP-Laadli Award for Gender Sensitivity. He is on the steering committee of the Impulse NGO Network Press Lab, which supports reporters who cover human trafficking. He is based in New Delhi.*

Indian police detain an opposition party worker during a February 2022 Mumbai protest accusing the Modi government of using Pegasus spyware to monitor political opponents, journalists, and activists. (AP/Rafiq Maqbool)

# For Mexican journalists, President López Obrador's pledge to curb spyware rings hollow

By Jan-Albert Hootsen

"Practically nothing." RíoDoce magazine editor Andrés Villarreal spoke with a sigh and a hint of resignation as he described what came of Mexico's investigation into the attempted hacking of his cell phone. "The federal authorities never contacted me personally. They told us informally that it wasn't them, but that's it."

Over five years have passed since Villarreal and Ismael Bojórquez, RíoDoce's co-founder and editor-in-chief, received the suspicious text messages that experts said bore telltale signs of Pegasus, the now notorious surveillance software developed by Israeli firm NSO Group. Just this month, a joint investigation by three Mexican rights groups and the University of Toronto's Citizen Lab found evidence of Pegasus infections on the devices of two Mexican journalists and a human rights defender between 2019 and 2021 – infiltration that occurred in spite of Mexican President Andrés Manuel López Obrador's 2018 promise to end illegal surveillance. (López Obrador denied on October 4 that his administration had used Pegasus against journalists or political opponents, saying, "if they have evidence, let them present it.")

The previous Mexican administration also denied using the technology on high-profile journalists, even after the Pegasus Project, a global consortium of investigative journalists and affiliated news outlets that investigated the use of the spyware, reported in 2021 that more than two dozen journalists in Mexico have been targeted with the spyware. Those named included award-winning investigative journalist Carmen Aristegui and Jorge Carrasco, the editor-in-chief of the country's foremost hard-hitting investigative magazine Proceso. Yet although the surveillance caused considerable outrage, almost nothing has changed since 2017, according to Villarreal, who spoke to CPJ from Sinaloa's capital, Culiacán.

In what CPJ has found to be by far the deadliest country for journalists in the Western Hemisphere, there remains no legal protection from intrusive surveillance, no recourse for its victims, and no repercussions for those in public office who facilitated the spying.

López Obrador's pledge to stop illegal surveillance was one of his first major undertakings after he took office in December 2018. Eleven months later, he assured Mexicans that the use of the Israeli spyware would be investigated. "From this moment I tell you that we're not involved in this. It was decided here that no one will be persecuted," he said.

But with just over two years left in office – Mexico's constitution allows presidents to serve only a single six-year term – journalists, digital rights groups, and human rights defenders say little has come of the president's promises. Not only has the investigation into the documented cases of illegal use of Pegasus shown no meaningful progress, the critics say, but also virtually nothing has been done to prevent authorities from continuing to spy.

"Unfortunately, the regulatory situation and the authorities' capacity to intercept communication have remained intact," said Luis Fernando García of Red en Defensa de los Derechos Digitales (R3D), a Mexico City-based digital rights group that supports reporters targeted with Pegasus. "There's very little transparency, very little publicly available information about the use of such technologies, which makes repetition a very real possibility."

CPJ contacted the office of President López Obrador's

spokesperson for comment before publication of the October report about the most recent infections but did not receive a reply.

NSO says it only sells Pegasus to government and law enforcement agencies to combat terrorism or organized crime. But investigative journalists report that in countries like Mexico non-state actors, including criminal groups, can also get their hands on these tools even if they are not direct clients. This poses a major threat to journalists and their sources across the region, where CPJ research has found that organized crime groups are responsible for a significant percentage of threats and deadly violence targeting the press. At least one Mexican journalist who was killed for his work, Cecilio Pineda Birto, may have been singled out for surveillance the month before his death.

Villarreal and Bojorquez received the first Pegasus-infected text messages just two days after Javier Valdez Cárdenas, Riodoce co-founder and a 2011 recipient of CPJ's International Press Freedom Award, was fatally shot on May 15, 2017, near the magazine's offices in northern Sinaloa state.

"Although it had all the hallmarks of Pegasus, it took us quite a while before we realized what was happening," Villarreal recalled. "We were in a very vulnerable state after Javier's death. It wasn't until approximately a month later, after contact with press freedom groups, that we realized that it was Pegasus."

A 2018 report by R3D, citing findings by Citizen Lab, stated that the likely source of Villarreal's surveillance was the Agency of Criminal Investigation, a now-defunct arm of the federal attorney general's office. Two autonomous federal regulators subsequently established that the attorney general's office used Pegasus illegally and violated privacy laws.

However, an ongoing federal investigation initiated under the previous government of President Enrique Peña Nieto has not led to any arrests of public officials. In December 2021, Mexican authorities requested the extradition from Israel of the former head of the criminal investigation agency, Tomás Zerón, in connection with

Mexican president Andres Manuel López Obrador, center, shown here at a military parade to commemorate Mexico's 212th anniversary of independence on September 16, 2022, denies that his administration has used Pegasus against journalists. (AFP/Rodrigo Arangua)

Ismail Bojórquez, co-founder and director of Riodoce, speaks with editors Andrés Villarreal and Judith Valenzuela at their office in Culiacan, Sinaloa state, Mexico on June 30, 2017. Bojorquez and Villarreal had received spyware-infected messages on their phones. (AP Photo/Enric Marti)

various investigations – reportedly including the Pegasus abuses – but that request has not yet been granted. (CPJ contacted the federal attorney general's office for comment on the extradition, but did not receive a reply.)

Concerningly, according to Proceso, investigators of the federal state comptroller revealed in the audit of the federal budget in October 2021 that the López Obrador administration had paid more than 312 million pesos (US $16 million) to a Mexican businessman who had facilitated the acquisition of Pegasus in the past.

The López Obrador administration has not publicly responded to Proceso's findings or the state comptroller's report, but the president did say during his daily press briefing on August 3, 2021, that there 'no longer existed a relationship' with the developer of Pegasus. The president's office had not responded to CPJ's request for comment on the payment by the time of publication.

Experts at R3D and Citizen Lab said Pegasus traces on a journalist's phone indicated they were hacked as recently as June 2021, just after they reported on alleged human rights abuses by the Mexican army for digital news outlet Animal Politico. The journalist was not named in reports of the incident.

"I don't think anything has changed," Villarreal said. "The risk continues to exist, but the government denied everything."

R3D, together with a number of other civil society groups, has also pushed hard for new legislation to curb the use of surveillance technologies by lobbying directly to legislators and via platforms like the Open Government Alliance. So far, the result has been disappointing. Even though López Obrador and his party, the Movement of National Regeneration (Morena), hold absolute majorities in both chambers of federal congress and have repeatedly acknowledged the need to end illegal surveillance, there has been no meaningful push for new legislation on either

the state or the federal level.

"There is indignation about surveillance, but my colleagues aren't picking the issue up," said Emilio Álvarez Icaza, an independent senator who has been outspoken about surveillance. "It's an issue that at least the Senate does not seem to really care about."

R3D's García warns that Pegasus is just a part of the problem. R3D and other civil society groups say they have detected numerous other technologies that were acquired by state and federal authorities even after the scope of Pegasus' use became clear.

"We've been able to detect the proliferation of systems that permit the intervention of telephones and there are publicly available documents that provide serious evidence that those systems have been used illegally," García said. "The [attorney general's office], for example, has acquired the capacity to conduct more than 100,000 searches of mobile phone data, but only gave clarity about 200 of them."

"Even with regulation, the Mexican justice state has a tremendous problem of lack of transparency and accountability. The entire system seems to have been constructed to protect public officials," said Ana Lorena Delgadillo, a lawyer and director of the Fundación para la Justicia, which provides legal support to Mexicans and Central Americans searching for 'disappeared' family members. "This is why I believe it's important that cases of this nature are ultimately brought to the Supreme Court, but it's hard to find people willing to litigate."

Villarreal said he will not be one of those afraid to speak out. "Ultimately we've left our cases in the hands of civil society organizations," he said. "Thing is, the spyware is just a new aspect of a problem that has always existed. The authorities have spied here, they will continue to do so. We have to adapt to the reality that we'll never know the extent of what's going on." ◆

*Jan-Albert Hootsen, CPJ's Mexico representative for the Americas program, works as a correspondent for Dutch newspaper Trouw, and regularly contributes to publications including Newsweek and RTL Nieuws. He is based in Mexico City.*

# In Morocco, journalists – and their families – still struggle to cope with spyware fears

By CPJ MENA Staff

Last July, when the Pegasus Project investigation revealed that imprisoned Moroccan journalist Soulaiman Raissouni was selected for surveillance by Israeli-made Pegasus spyware, the journalist could only laugh.

"I was so sure," his wife Kholoud Mokhtari said Raissouni told her from prison.

Raissouni is one of seven local journalists named by the Pegasus Project – an investigative consortium of media organizations – as a potential or confirmed target of Pegasus spyware. The news only validated what Moroccan's journalist community had long suspected: that the state's vast intelligence apparatus has been monitoring some journalists' every move.

Moroccan journalists were among the first worldwide to complain of the use of spyware against reporters, pointing to digital surveillance as early as 2015. In 2019 and 2020, Amnesty International announced the findings of forensic analyses confirming that Pegasus had been used on the phone of at least two Moroccan journalists, Omar Radi and Maati Monjib. Subsequent state action against some of the surveilled journalists underscored the ongoing threat to Morocco's independent media – and reinforced CPJ's conclusion that spyware attacks often are precursors to other press freedom violations.

Both Raissouni and Radi are imprisoned in Morocco for what family and colleagues describe as trumped up sex crimes charges. Taoufik Bouachrine, another journalist whom the Pegasus Project said was targeted with the spyware, is imprisoned on similar charges.

The Pegasus Project was unable to analyze the phones of all of those named as surveillance targets to confirm the infection and the Moroccan government has repeatedly denied ever using Pegasus. However, many of the three journalists' private pictures, videos, texts, and phone calls, as well as those belonging to family members, were published in pro-government newspapers and sites like Chouf TV, Barlamane.com, Telexpresse, and then later used as evidence against the journalists in court.

Bouachrine, former editor-in-chief of local independent newspaper Akhbar al-Youm, was arrested in February 2018, and is serving a 15-year prison sentence on numerous sexual assault and human trafficking charges. His wife, Asmae Moussaoui, told CPJ in a phone call in May 2022 that she believes she was surveilled, too.

In April 2019, Moussaoui said she called a private Washington, D.C.-based communications firm to help her run ads in U.S. newspapers about Bouachrine's case, hoping that the publicity might aid efforts to free her husband. The next day, Barlamane published a story alleging that Moussaoui paid tens of thousands of euros to the firm, using money the journalist allegedly earned through human trafficking activities. Human Rights Watch describes Barlamane as being "closely tied with security services."

Suspecting she was being monitored, Moussaoui turned to one of her husband's lawyers, who suggested the pair "pull a prank" that would help them detect whether authorities were indeed spying on her. The lawyer "called me and proposed that we speak with Taoufik's alleged victims to reconcile, which we did not really intend to do. The next day, tabloids published an article saying that our family is planning to bribe each victim with two million


The mother of imprisoned Moroccan journalist Omar Radi holds a banner showing her son's image during a demonstration in his support in Casablanca on September 22, 2020. Radi is among several Moroccan journalists targeted with spyware. (AFP/Fadel Senna)

dirhams [about $182,000] so they drop the case. I became very sure [of the surveillance] then," Moussaoui told CPJ.

Moroccan journalist and press freedom advocate Maati Monjib, co-founder of the Moroccan Association for Investigative Journalism (AMJI), had a similar experience. Monjib was arrested in December 2020 and sentenced to a year in prison the following month after he was convicted of endangering state security and money laundering fraud. The latter charge stems from AMJI's work helping investigative journalists apply for grants, Monjib told CPJ in a phone call.

"During one of our meetings at AMJI in 2015, I mentioned that we need to look for grants to support more journalists. The next day, one of the tabloids published a story claiming that Maati Monjib is giving 5,000 euros [$4,850] to every journalist who criticizes the general director of the national security. This is a proof that they were listening to our meeting," said Monjib.

The revelations have forced journalists and their family members to take precautions against surveillance – no easy task given the difficulty of detecting spyware infection without forensic help. "[Raissouni] told me to try to be safe, so I am trying my best," Mokhtari, Raissouni's wife, told CPJ.

"Other than the usual precautions I take to protect my phone, I regularly update it and I never keep any personal pictures or important messages or emails on it," she said. "I also buy a new phone every three months and destroy the old one, which has taken a financial toll on my family. But honestly you can't escape it. The most tech-savvy person I know is our friend Omar Radi. He took all the necessary precautions against hacking, and they still managed to infect his devices."

Monjib brings his devices to tech experts almost daily to check for bugs and to clean them, he told CPJ, adding that he also never answers phone calls, only uses the

encrypted Signal messaging app, and always speaks in code.

Aboubakr Jamai, a prominent Moroccan journalist and a 2003 CPJ International Press Freedom Award winner, was selected for surveillance with Pegasus in 2018 and 2019 — and confirmed as a target in 2019 — even though he has been living in France since 2007, according to the Pegasus Project. He believes that the Moroccan government is to blame for the spyware attacks, and that the surveillance has effectively ensured the end of independent journalism in the country, he told CPJ in a phone call.

"For years now, there haven't been any independent media or journalism associations," said Jamai. What's left now is a handful of individuals who have strong voices and choose to echo it using some news websites, but mainly social media platforms."

CPJ emailed the Moroccan Ministry of Interior in September for comment but did not receive any response.

Still, Jamai – who gave no credence to the government's earlier denials of Pegasus use – did see one positive result from the spyware disclosures. "It publicly exposed Morocco's desperation and the extent to which it is willing to go to silence journalists," he said. "Now the whole world knows that the Moroccan state is using Pegasus to spy on journalists." ◆

# David Kaye: Here's what world leaders must do about spyware

By David Kaye

In late June, the general counsel of NSO Group, the Israeli company responsible for the deeply intrusive spyware tool, Pegasus, appeared before a committee established by members of the European Parliament (MEPs). Called the PEGA Committee colloquially, the Parliament established it to investigate allegations that EU member states and others have used "Pegasus and equivalent spyware surveillance software." This was to be PEGA's first major news-making moment, a response to the very public scandals involving credible allegations of Pegasus use by Poland, Hungary and, most recently, Spain.

The hearing started unsurprisingly enough. Chaim Gelfand, the NSO Group lawyer, laid out the company line that Pegasus is designed for use against terrorists and other criminals. He promised that the company controlled its sales, developed human rights and whistleblowing policies, and took action against those governments that abused it. He wanted to "dispel certain rumors and misconceptions" about the technology that have circulated in "the press and public debate." He made his case.

Then, surely from NSO Group's perspective, it went downhill. MEP after MEP asked specific questions of NSO Group. For instance: if Pegasus is sold only to counter terrorism or serious crime, how did it come to be used in EU member states? How did it come to be used to eavesdrop on staffers at the European Commission, another public allegation? Can NSO provide examples of when it terminated contracts because a client misused Pegasus? Can NSO clarify what data it has on its clients' uses of Pegasus? How does NSO Group know when the technology is "abused"? More personally: *How come you spied on me?*

MEPs were angry. Increasingly their questions became more intense, more personal, more laced with moral and legal outrage. And this tenor only deepened over the course of the hearing, as the NSO lawyer stumbled through his points and regularly resorted to the line that he could not speak to specific examples, cases or governments. Few, if any, seemed persuaded by the NSO Group claim that it has no insight into the day-to-day use of the spyware by the "end-user". To the contrary, the PEGA hearing ended with one thing clear: NSO Group faces not only anger but the

David Kaye addresses a press conference in Mexico City, on December 4, 2017. At the time, he investigated surveillance as the U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. (AFP/Ronaldo Schemidt)

reality of an energized set of legislators.

More than a year after release of the Pegasus Project, the global reporting investigation that disclosed massive pools of potential targets for Pegasus surveillance, the momentum for action against spyware like Pegasus is gathering steam.

In 2019, in my capacity as a U.N. Special Rapporteur, I issued a report to the United Nations Human Rights Council that surveyed the landscape of the private surveillance industry and the vast human rights abuses it facilitates, calling for a moratorium on the sale, transfer and use of such spyware. At the time, few picked up the call. But today, with extensive reporting of the use of spyware tools against journalists, opposition politicians, human rights defenders, the families of such persons, and others, the tide seems to be turning against Pegasus and spyware of its ilk.

The U.N. High Commissioner for Human Rights, several U.N. special rapporteurs, the leaders of major human rights organizations, and at least one state, Costa Rica, have joined the call for a moratorium. The Supreme Court of India is pursuing serious questions about the government's use of Pegasus. The United States Department of Commerce placed NSO Group and another Israeli spyware firm on its list of restricted entities, forbidding the U.S. government from doing any business with them. Apple and Facebook's parent company Meta have sued NSO Group for using their infrastructure to hack into individual phones.

All of these steps suggest not only momentum but the elements of a global process to constrain the industry. They need to be transformed into a long-term strategy to deal with the threats posed to human rights by intrusive, mercenary spyware. State-by-state responses, or high-profile corporate litigation, will generate pain for specific companies and begin to set out the normative standards that should apply to surveillance technologies. But in order to curb the industry as a whole, a global approach will be necessary.

In principle, spyware with the characteristics of Pegasus – the capability to access one's entire device and data connected to it, without discrimination, and without constraint – *already* violates basic standards of necessity and proportionality under international human rights law. On that ground alone, it's time to begin speaking of not merely a moratorium but a ban of such intrusive technology, whether provided by private or public actors. No government should have such a tool, and no private company should be able to sell such a tool to governments or others.

In the land of reality, however, a ban will not take place immediately. Even if a coalition of human rights-friendly governments could get such negotiations toward a ban off the ground, it will take time.

Here is where bodies like the European Parliament and its PEGA Committee – and governments and parliamentarians around the world – can make an immediate difference. They should start to discuss a permanent ban while also entertaining other interim approaches: stricter global export controls to limit the spread of spyware technology; commitments by governments to ensure that their domestic law enables victims of spyware to bring suits against perpetrators, whether domestic or foreign; and broad agreement by third-party companies, such as device manufacturers, social media companies, security entities and others, to develop a process for notification of spyware breaches especially to users and to one another.

Some of this would be hard to accomplish. It's not as if the present moment, dominated as it is by tensions like Russian aggression against Ukraine, is conducive to international negotiations. Some steps could be achieved by governments that should be concerned about the spread of such technologies, already demonstrated by U.S. and European outrage. Either way, governments and activists can begin to lay the groundwork, defining the key terms, highlighting the fundamental illegality of spyware like Pegasus, taking steps in domestic law to ensure strict controls on export and use.

There is precedent for such action in the global movement to ban landmines in the 1990s, which started with little hope of achieving a ban, focused instead on near-term controls. Ultimately human rights activists and like-minded governments were able to hammer out the Ottawa Convention to ban and destroy anti-personnel landmines in 1997. It is, at least, a process that activists and governments today could emulate and modify.

Human rights organizations and journalists have done the work to disclose the existence of a major threat to freedom of expression, privacy, and space for public participation. It is now the duty of governments to do something about it. ◆

*David Kaye is a clinical professor of law at the University of California, Irvine, and a former U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. The views expressed here are his own.*

# CPJ recommendations to protect journalists against spyware

The arbitrary or unlawful use of spyware technologies violates human rights and causes direct damage to journalists and their ability to report freely and safely. These recommendations are necessary to protect journalists and their sources.

## FOR ALL GOVERNMENTS

- Implement an immediate moratorium on the development, export, sale, transfer, servicing, and use of spyware technologies until governments have enacted robust regulations that guarantee its use in line with international human rights standards.
- Bar government agencies from purchasing or licensing the export of spyware technology from companies that sell to governments with a track record of attacking press freedom and/or journalists, or that lack mechanisms to prevent their clients from unlawfully targeting the press.
- Commit to not using spyware technology against journalists and pursue efforts to make it explicitly illegal in national legislation.
- Establish accountability and remedy mechanisms in documented cases of abuse against the media
- Where governments continue to engage in the use or sale of this technology, require public reporting and consultation about spyware purchases and exports
- Use targeted actions – including visa and economic sanctions and export control listings – to hold accountable those who have spied or facilitated spying on journalists through the sale or use of spyware, and to deter future spying.
- If not a member, join the Export Controls and Human Rights Initiative, an international effort to codify rights-respecting policy approaches to surveillance technology exports, and use it to build consensus for global action through concrete action.

## FOR THE U.S. GOVERNMENT

- Comply with the Congressional requirement to create a list of companies known to sell such spyware to countries with a record of using it unlawfully or with poor human rights records. *[Note: the State Department was required to do this by National Defense Authorization Act 2021 but hasn't complied yet. State said they are working on it.]*
- Continue to use the Department of Commerce's (DoC) Entity List for Malicious Cyber Activities to impose export controls on spyware-producing companies, such as was done with NSO Group.
- Stringently enforce a new DoC rule establishing controls on the export, reexport, or transfer of items that can be used to spy on journalists.
- Ensure U.S. businesses are complying with the State Department's September 2020 Guidance on "Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities."
- Congress should adopt the Surveillance Technologies Disclosure Rule, which would require companies to conduct human rights due diligence and provide transparency in the surveillance technologies' supply chain.

- Congress should adopt the Foreign Advanced Technology Surveillance Accountability Act, which would require the U.S. State Department to report on the wrongful use of surveillance technologies in the annual Country Reports on Human Rights Practices.

## FOR EUROPEAN UNION INSTITUTIONS

- EU member states should fully implement the European Parliament regulation on the export of dual-use surveillance technology by EU-based companies and prevent the export of this technology from harming human rights in countries where journalists are targeted and under surveillance because of their work.
- The European Parliament's Committee of Inquiry into Pegasus and equivalent spyware should conduct full and independent investigations into all allegations of abuse of Pegasus in EU member states and in third countries. The committee should issue ambitious and robust recommendations to EU member states, and the institutions, with a structured plan for continued scrutiny and timely monitoring to ensure all recommendations are implemented in full.
- EU member states should fully and independently investigate all national reports that Pegasus has been used to spy on journalists, providing full access to remedy for journalists targeted, including guarantees of non-repetition and restitution.
- The European Commission should assess the extent to which the Pegasus revelations have breached EU law, seek all sanctions against violating member states, including infringement procedures, and consider its own competencies to defend EU citizens against such abuse in the future.

## FOR COMPANIES

- Embrace corporate accountability by making  a public commitment to press freedom and protecting journalists and media outlets from covert surveillance.
- Prohibit clients from deploying technology to spy on journalists by inserting explicit terms in contracts and licenses.
- Revoke access to spyware when abuse is detected, and report abuse to affected individuals, relevant authorities, and oversight bodies.
- Establish procedures to review complaints and support human rights monitors investigating allegations of abuse involving specific products.

## FOR INTERNATIONAL ORGANIZATIONS

- Consult with civil society, report on the use of spyware against journalists around the world, and raise cases with governments.
- Use human rights review mechanisms, including the Universal Periodic Review, and related processes to ensure that commitments to limit the abusive use of surveillance technologies, including spyware, translate to appropriate action, laws and policies that align with international human rights standards on targeted surveillance.
- Promote public debate about the abusive use of spyware and encourage member states to adopt policies and laws to stem the problem by requiring corporate actors to respect human rights and implement measures as prescribed by the United Nations Guiding Principles on Business and Human Rights.

See CPJ's 2021 policy brief for summarized recommendations.

Defending Journalists Worldwide

cpj.org
@pressfreedom
fb.com/committeetoprotectjournalists