RON DEIBERT

Protecting Society from Surveillance Spyware

Days after Mexican journalist Javier Valdez Cárdenas was gunned down in the streets, most likely by a drug cartel, his wife Griselda Triana's cell phone was targeted with a powerful, government-grade spyware. After exiled Rwandan political opposition figure Faustin Rukundo's name appeared on a widely circulated list entitled "Those who must be killed immediately," he learned that his phone had been targeted with the same spyware. Shortly after exiled Saudi activist Omar Abdulaziz discovered that his phone was hacked, he alerted his close confidant, journalist and Washington Post columnist Jamal Khashoggi, that their private conversations had likely been intercepted for months by Saudi security services. The day after Abdulaziz's story was made public, Khashoggi was murdered in the Saudi consulate in Istanbul, Turkey. Later, retrospective forensic analysis showed that the phone of Khashoggi's fiancé, Hatice Cengiz, had also been hacked with the same spyware.

At the Citizen Lab, a University of Toronto-based research group that undertakes evidence-based research on targeted digital espionage, we have identified hundreds of people whose phones have been targeted or hacked in ways such as those described above. The common denominator? A powerful government-grade spyware manufactured by the Israel-based surveillance company, NSO Group. Its flagship product, called Pegasus, is used by NSO Group's government clients to monitor the devices that are hacked, including intercepting all emails and texts (even those that are encrypted), turning on the audio and video applications, and silently tracking the location of targets.

What is truly daunting to contemplate, however, is that NSO Group is but one among many companies in a growing marketplace for this type of surveillance technology. The list of mercenary spyware firms that the Citizen Lab alone has reported on include Hacking Team, Gamma Group (parent company of the FinFisher surveillance software), Candiru, Cyberbit, Circles, and Cytrox. Dozens of other companies whose wares have yet to be identified are no doubt flourishing undetected—in spite of the continuous investigations of organizations like the Citizen Lab and Amnesty International. This multibillion dollar industry is providing a new kind of "despotism-as-a-service," enabling buyers to reach across borders and undermine their adversaries. Very little stands in the way, since there are presently no international regulations governing the sale or transfer of commercial spyware. This highly lucrative industry is flourishing in what is largely an ungoverned realm.

In the short run, digital technologies and social media appeared to empower transnational civil society, particularly during events such as the 2011 Arab Spring. But over time the power dynamic has flipped entirely in favor of illiberal governments and their security agencies, helping to fuel the spread of a new kind of digital authoritarianism that crosses international borders. The effects are disturbing. The Citizen Lab has interviewed activists, refugees, and immigrants who fled their home countries in fear of persecution only to have their devices hacked while abroad. This new digital repression can have severe psychological impacts. Even if someone hasn't been hacked themselves, the mere awareness of this type of hacking creates a widespread and debilitating climate of fear, paranoia, and self-censorship.

A growing market for mercenary spyware

As mobile technology has become more popular, the market for spyware has expanded. The industry has arisen in part to take advantage of the opportunities presented by today's always-on, digitally networked society. Almost everyone carries around a mobile device that connects to a worldwide web of digital information. But the "move fast and break things" philosophy that underpins innovation in the digital economy has produced an ecosystem that is invasive by

design, insecure, poorly regulated, and easily exploited. Although people are used to thinking of social media and the devices they use to connect to the web as windows on the world, they are also highly convenient windows into users' lives for those with the resources and capabilities to peer inside.

Many firms now orbit around the social media and digital technological environment, vacuuming up revealing information about personal lives, social relationships, habits, and location. Most do so for the relatively benign purpose of targeted advertising. But some specialize in lucrative contracts with defense, law enforcement, and intelligence agencies. They offer services including location tracking, mobile forensics, facial recognition, and more. The most invasive are those that provide spyware such as Pegasus, which enables clients to break inside and monitor everything on a target's device. Behind the shell companies, public relations firms, lawyers, and equity funds that surround companies like NSO Group are organizations that offer a very basic service: hacking for hire.

Government security agencies have had, for decades, a growing interest in and appetite for digital surveillance. At first, only the most well-resourced, such as the US National Security Agency (NSA), could develop sophisticated in-house capabilities. That started to change shortly after the Arab Spring, when some governments sought out ways to counter digitally empowered civil movements challenging repressive regimes. Thanks to the growing number of surveillance firms, governments around the world—including those lacking domestic technical resources and capabilities of their own—discovered that they could effectively purchase their own "NSA" off the shelf. In governments that lack appropriate safeguards over their security agencies or are authoritarian, corrupt, or illiberal, abuses naturally have followed. The industry markets itself as providing governments with the means to investigate serious matters of crime and terrorism, but left unchecked their products have become a convenient tool for undermining public accountability and political opposition, both at home and abroad.

Identifying the culprits

The Citizen Lab focuses on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security. We use a mixed methods approach to research, combining practices from political science, law, computer science, and area studies. We seek to unearth evidence of abuses of power or risks to civil society that happen in the digital realm through careful, peer-reviewed, evidence-based analysis. Although we work on many topics, our research into targeted espionage has been at once the most disturbing and impactful.

In March 2021, for example, Citizen Lab researchers examined the phone of a Saudi activist and determined that it had been hacked with a particularly powerful version of Pegasus software known as a "zero-click" exploit. (Citizen Lab cannot disclose the identity of the individual whose phone was hacked without their explicit permission.) Rather than infecting a device by tricking a target into clicking on a malicious link or attachment contained in an email or text message, a zero-click exploit requires no interaction with the target and leaves no visible evidence of tampering. A government operator armed with Pegasus merely sends data over the network to a target's device and, assuming it's running an operating system vulnerable to this type of exploitation, the spyware silently activates and the phone is surreptitiously taken under the spyware's total control.

This particular exploit was also a "zero day" vulnerability, which is industry jargon for a software flaw that even the vendor—which in this case was Apple—is unaware of. NSO Group employs a large number of highly trained engineers who scour operating systems and applications looking for software vulnerabilities they can exploit, and they treat those vulnerabilities as NSO Group's proprietary data. At the Citizen Lab, on the other hand, we responsibly disclose them in the interests of public safety. The exploit we captured on the Saudi activist's phone was functional against all of the latest Apple iOS, MacOS, and WatchOS systems at the time. Based on Citizen Lab's investigation and disclosure, in September 2021 Apple pushed out an emergency security patch to all of its 1.6 billion customers. Two months later, Apple announced that it was filing a legal complaint in US courts against NSO Group, referring to the defendants as "amoral 21st century mercenaries." Apple further noted that the Citizen Lab's disclosure of the spyware was critical in enabling the company to track down and neutralize NSO Group's exploitation of Apple's infrastructure and customers.

For the moment, one mercenary spyware company's arsenal was disrupted. However, fresh vulnerabilities will no doubt soon be identified and exploited by other spyware firms, as long as the market for this type of hacking technology continues unchecked. The reality is that regardless of how much effort tech platforms put into carefully coding their operating systems, well-resourced surveillance companies will inevitably find some flaw that can be exploited—particularly when the tech industry's incentives tend to prioritize innovation and product development at the expense of security.

What is to be done?

Reflecting the urgency of the problem, some have advocated for an immediate worldwide moratorium on the sale and transfer of commercial spyware until safeguards are in place. But such a call is very unlikely to be implemented in practice. Illiberal governments are the least likely to cooperate, since

they benefit the most from the existing Wild West marketplace. But even liberal democracies benefit from and contract with surveillance technology vendors for law enforcement and intelligence purposes, as the Edward Snowden disclosures showed. As long as even one government supports the industry, a global moratorium will remain little more than a rhetorical plea.

But there are shorter-term measures to punish offenders and mitigate harms that could and should be taken by liberal democracies in support of the rule of law and human rights right now. First, these governments should be more transparent and accountable when it comes to their own procurements, treating surveillance vendors with the same level of seriousness as some do the sale of advanced weaponry. Governments should mandate that they will only contract with surveillance firms that meet a specific threshold of due diligence around human rights compliance, which can be measured with real data and independent oversight. Such an "allow/deny" list of vendors would not run the worst offenders out of business entirely, but it would marginalize them from some important marketplaces.

Second, governments could tighten export controls to ensure surveillance vendors based in their own jurisdictions meaningfully comply with standards such as those outlined in the UN Guiding Principles for Human Rights. While the European Union has made considerable strides in this direction, other governments have not and should do more. Canada, for example, is home to a growing number of surveillance and dual-use technology firms implicated in sales to regimes that violate human rights. Yet there is virtually no government oversight regulating these companies' sales abroad; in fact, the Canadian government has helped support those sales through trade exhibitions sponsored by Canadian government ministries. Once again, regulatory measures wouldn't eliminate the harms around the industry as a whole, but it would set a precedent for others to follow.

Third, governments could use existing regulatory measures to hold the worst offenders in the mercenary spyware industry legally accountable. In a dramatic development in November 2021, the US Department of Commerce added NSO Group, Candiru, and several other mercenary spyware firms to its designated "Entity List" of blacklisted companies. Only a few weeks later, reports surfaced that several US diplomats were notified by Apple that their phones had been hacked with Pegasus—which supported the Commerce Department's observation that the activities of mercenary surveillance firms are "contrary to the national security or foreign policy interests of the United States." The Entity List designation effectively prohibits US organizations from doing business with NSO Group without a special exemption. More broadly, it sends a loud signal to the world that the services of such companies are a menace to human rights and even national security. If other governments followed the United States' lead, strong restraints would be placed around companies like NSO Group, hindering their usual methods of doing business. These actions would also undoubtedly scare off investors and other backers, providing an incentive for mercenary spyware firms to change their behavior. For example, shortly after the Entity List designation, the credit rating agency Moody's downgraded NSO Group and warned that it was at risk of defaulting on its loans. Speculation is now circulating that the firm may even fold entirely.

Lastly, legislation could open avenues for private litigation, allowing victims of targeted espionage to hold both governments and companies accountable. Currently, governments hide behind foreign immunity provisions, and vendors may avoid responsibility for harm caused by their products when used by government clients. Creating specific laws that would allow victims to sue both vendors and government clients in specific jurisdictions would increase liabilities for companies, investors, and government operators alike. Likewise, technology platforms whose infrastructure has been exploited by mercenary spyware firms could litigate against those companies for violation of their terms of service or other damages.

Notably, in October 2019, WhatsApp and Facebook filed a complaint against NSO Group in the Northern District of California. These companies are seeking injunctive relief and damages pursuant to the Computer Fraud and Abuse Act and the California Comprehensive Data Access and Fraud Act. They are also suing for breach of contract and other offenses. In November 2021, Apple filed a similar complaint against NSO Group in the same district court. It also pledged to donate financing and resources to groups involved in countersurveillance research and advocacy. Should avenues for legal redress open, setting a precedent for significant financial penalties may make mercenary spyware firms and their investors more risk averse.

The problem of mercenary spyware is difficult, with no one simple policy or technological solution. And yet in the absence of action, spyware is evolving to become more sophisticated while the abuses and harms continue to mount worldwide. The proliferation of this type of despotism-as-a-service has become a major threat to liberal democracy, civil society, and human rights. The time has come to rein it in.

Ron Deibert *is the founder and director of the Citizen Lab at the University of Toronto's Munk School of Global Affairs and Public Policy.*