The Autocrat in Your iPhone

How Mercenary Spyware Threatens Democracy

RONALD J. DEIBERT

In the summer of 2020, a Rwandan plot to capture exiled opposition leader Paul Rusesabagina drew international headlines. Rusesabagina is best known as the human rights defender and U.S. Presidential Medal of Freedom recipient who sheltered more than 1,200 Hutus and Tutsis in a hotel during the 1994 Rwandan genocide. But in the decades after the genocide, he also became a prominent U.S.-based critic of Rwandan President Paul Kagame. In August 2020, during a layover in Dubai, Rusesabagina was lured under false pretenses into boarding a plane bound for Kigali, the Rwandan capital, where government authorities immediately arrested him for his affiliation with an opposition group. The following year, a Rwandan court sentenced him to 25 years in prison, drawing the condemnation of international human rights groups, the European Parliament, and the U.S. Congress.

RONALD J. DEIBERT is Professor of Political Science and Director of the Citizen Lab at the University of Toronto's Munk School of Global Affairs and Public Policy.

Illustration by Daniel Stolle

Less noted at the time, however, was that this brazen cross-border operation may also have employed highly sophisticated digital surveillance. After Rusesabagina's sentencing, Amnesty International and the Citizen Lab at the University of Toronto, a digital security research group I founded and direct, discovered that smartphones belonging to several of Rusesabagina's family members who also lived abroad had been hacked by an advanced spyware program called Pegasus. Produced by the Israel-based NSO Group, Pegasus gives an operator near-total access to a target's personal data. Forensic analysis revealed that the phone belonging to Rusesabagina's daughter Carine Kanimba had been infected by the spyware around the time her father was kidnapped and again when she was trying to secure his release and was meeting with high-level officials in Europe and the U.S. State Department, including the U.S. special envoy for hostage affairs. NSO Group does not publicly identify its government clients and the Rwandan government has denied using Pegasus, but strong circumstantial evidence points to the Kagame regime.

In fact, the incident is only one of dozens of cases in which Pegasus or other similar spyware technology has been found on the digital devices of prominent political opposition figures, journalists, and human rights activists in many countries. Providing the ability to clandestinely infiltrate even the most up-to-date smartphones—the latest "zero click" version of the spyware can penetrate a device without any action by the user—Pegasus has become the digital surveillance tool of choice for repressive regimes around the world. It has been used against government critics in the United Arab Emirates (UAE) and pro-democracy protesters in Thailand. It has been deployed by Mohammed bin Salman's Saudi Arabia and Viktor Orban's Hungary.

But the use of spyware is hardly limited to the world's authoritarians. As researchers have revealed, over the past decade many democracies, including Spain and Mexico, have begun using spyware, as well, in ways that violate well-established norms of human rights and public accountability. U.S. government documents disclosed by *The New York Times* in November 2022 show that the FBI not only acquired spyware services from NSO, possibly for counterintelligence purposes, but also contemplated deploying them, including on U.S. targets. (An FBI spokesperson told the *Times* that "there has been no operational use of the NSO product to support any FBI investigation.")

The advent of advanced spyware has transformed the world of espionage and surveillance. Bringing together a largely unregulated industry with an invasive-by-design digital ecosystem in which smartphones and other personal devices contain the most intimate details of people's lives, the new technology can track almost anyone, anywhere in the world. Governments have taken notice. For Israel, which approves export licenses for NSO Group's Pegasus, the sale of spyware to foreign governments has brought new diplomatic clout in countries as disparate as India and Panama; a *New York Times* investigation found that NSO deals helped Israeli Prime Minister Benjamin Netanyahu seal the Abraham Accords with Bahrain, Morocco, and the UAE. In turn, client states have used Pegasus against not only opposition groups, journalists, and nongovernmental organizations (NGOs) but also geopolitical rivals. In 2020 and 2021, the Citizen Lab discovered that several devices belonging to officials in the United Kingdom's Foreign Commonwealth and Development Office had been hacked with Pegasus, and that a client of NSO Group in the UAE had used the spyware to infiltrate a device located at 10 Downing Street, the residence of the British prime minister. In November 2021, the tech giant Apple notified 11 staff members of the U.S. embassy in Uganda that their iPhones had been hacked with Pegasus.

With spyware, governments can stop protests before they occur.

In response to these revelations, spyware firms have generally denied responsibility for their clients' abuses or have declined to comment. In a statement to *The New Yorker* in April 2022, NSO Group said, "We have repeatedly cooperated with governmental investigations, where credible allegations merit, and have learned from each of these findings and reports and improved the safeguards in our technologies." The Israeli company has also said that its technology is designed to help governments investigate crime and terrorism. But advanced spyware has now been implicated in human rights violations and interstate espionage in dozens of countries, and spyware companies have few legal obligations or incentives for public transparency or accountability. NSO Group has not provided any specific information to counter the Citizen Lab's detailed evidence of abuses.

The consequences of the spyware revolution are profound. In countries with few resources, security forces can now pursue high-tech operations using off-the-shelf technology that is almost as easy to acquire as headphones from Amazon. Among democracies, the technology has become an irresistible tool that can be deployed with little oversight; in the last year alone, security agencies in at least four

European countries—Greece, Hungary, Poland, and Spain—have been implicated in scandals in which state agencies have been accused of deploying spyware against journalists and political opposition figures. A global market for spyware also means that forms of surveillance and espionage that were once limited to a few major powers are now available to almost any country, and potentially to even more private firms. Left unregulated, the proliferation of this technology threatens to erode many of the institutions, processes, and values on which the liberal international order depends.

WE WILL SPY FOR YOU

The spyware revolution has emerged as a byproduct of a remarkable convergence of technological, social, and political developments over the past decade. Smartphones and other digital devices are vulnerable to surveillance because their applications often contain flaws and because they continually transmit data through insecure cellular and Internet networks. Although manufacturers of these technology platforms employ engineers to find and patch vulnerabilities, they tend to prioritize product development over security. By discovering and weaponizing "zero days"—software flaws that are unknown to their designers—spyware firms exploit the inherent insecurity of the digital consumer world.

But the extraordinary growth of the spyware market has also been driven by several broader trends. First, spyware takes advantage of a global digital culture that is shaped around always-on, always-connected smartphones. By hacking a personal device, spyware can provide its operators with a user's entire pattern of life in real time. Second, spyware offers security agencies an elegant way to circumvent end-to-end encryption, which has become a growing barrier to government mass surveillance programs that depend on the collection of telecommunications and Internet data. By getting inside a user's device, spyware allows its operators to read messages or listen to calls before they have been encrypted or after they have been decrypted; if the user can see it on the screen, so can the spyware. A third factor driving the industry's growth has been the rise of digitally enabled protest movements. Popular upheavals such as the color revolutions in former Soviet states in the first decade of this century and the Arab Spring in 2010–11 took many autocrats by surprise, and the organizers often used phones to mobilize protesters. By offering an almost godlike way to get inside activist networks, spyware has opened

HOW WILL *you* CHANGE *the* WORLD?

Georgetown's School of Foreign Service — the oldest school of international affairs in the United States — prepares students to lead in business, tech, development, national security and government. We provide unparalleled access to renowned scholars and faculty with real-world experience who empower students to make an impact at a critical moment in global affairs.

Join our community of changemakers. Join SFS.

SFS | GEORGETOWN UNIVERSITY
Walsh School *of* Foreign Service

SFS.GEORGETOWN.EDU

Graduate and Undergraduate Degrees in International Affairs

up a powerful new method for governments to monitor dissent and take steps to neutralize it before large protests occur.

Finally, the spyware industry has also been fueled by the growing privatization of national security. Just as governments have turned to private contractors for complicated or controversial military operations, they have discovered that they can outsource surveillance and espionage to better-equipped and less visible private actors. Like soldiers of fortune, advanced spyware companies tend to put revenues ahead of ethics, selling their products without regard to the politics of their clients—giving rise to the term "mercenary spyware"—and like military contractors, their dealings with government security agencies are often cloaked in secrecy to avoid public scrutiny. Moreover, just as military contractors have offered lucrative private-sector careers for veterans of military and intelligence agencies, spyware firms and government security services have been building similarly mutually beneficial partnerships, boosting the industry in the process. Many senior members of NSO Group, for example, are veterans of Israeli intelligence, including the elite Military Intelligence Directorate.

Although lack of transparency has made the mercenary spyware industry difficult to measure, journalists have estimated it to be worth about $12 billion per year. Before recent financial setbacks brought on by a growing number of lawsuits, NSO Group was valued at $2 billion, and there are other major players in the market. Many companies now produce sophisticated spyware, including Cytrox (founded in North Macedonia and now with operations in Hungary and Israel), Israel-based Cyberbit and Candiru, Italy-based Hacking Team (now defunct), and the Anglo-German Gamma Group. Each of these firms can hypothetically serve numerous clients. Governments that appear to have used Cytrox's Predator spyware, for example, include Armenia, Egypt, Greece, Indonesia, Madagascar, and Serbia. In 2021, Mexico's secretary of Security and Public Safety, Rosa Icela Rodríguez, said that previous Mexican administrations had signed multiple contracts with NSO Group, totaling $61 million, to buy Pegasus spyware, and as Mexican and international researchers have shown, the government has kept using Pegasus despite the present leadership's public assurances that it would not. (In October 2022, Mexican President Andrés Manuel López Obrador denied the findings, stating that his administration was not using the spyware against journalists or political opponents.)

On the basis of such lucrative deals, spyware firms have enjoyed backing from major private equity funds, such as the San Francisco firm Francisco Partners and the London-based Novalpina Capital, thus bolstering their resources. Francisco Partners, which had a controlling stake in NSO Group for five years, told Bloomberg News in 2021, "[We are] deeply committed to ethical business practices, and we evaluate all our investments through that lens." Novalpina, which together with NSO's founders acquired Francisco Partners' stake in 2019, said it would bring the spyware firm "in full alignment with UN guiding principles on business and human rights," but revelations of abuses of Pegasus have continued, and correspondence published by *The Guardian* in 2022 indicated that Novalpina sought to discredit NSO Group's critics, including this author. (Lawyers for Novalpina told *The Guardian* that these were "tenuous and unsubstantiated allegations.") After a dispute between Novalpina's founding partners, the firm lost its controlling stake in NSO Group in 2021.

But the spyware industry also includes far less sophisticated firms in countries such as India, the Philippines, and Cyprus. As the surveillance equivalent of strip-mall phone repair shops, such outfits may lack the ability to identify zero days, but they can still accomplish objectives through simpler means. They may use credential phishing—using false pretenses, often via email or text message, to obtain a user's digital passwords or other sensitive personal information—or they may simply purchase software vulnerabilities from other hackers on the black market. And these smaller firms may be more willing to undertake illegal operations on behalf of private clients because they are located outside the jurisdiction in which a victim resides or because enforcement is lax.

It is hard to overestimate the reach and power of the latest commercial spyware. In its most advanced forms, it can silently infiltrate any vulnerable device anywhere in the world. Take the zero-day, zero-click exploit that Citizen Lab researchers discovered in 2021 on a Pegasus-infected iPhone. Using the exploit, which researchers called ForcedEntry, a spyware operator can surreptitiously intercept texts and phone calls, including those encrypted by apps such as Signal or WhatsApp; turn on the user's microphone and camera; track movements through a device's GPS; and gather photos, notes, contacts, emails, and documents. The operator can do almost anything a user can do and more, including reconfigure the device's security settings and acquire the digital tokens that are used to securely access cloud accounts so that surveillance on a target can continue even after the exploit has been removed from a device—all without the target's awareness. After the Citizen Lab shared Pegasus's ForcedEntry with analysts at Apple and Google, Google's analysts described it as "one of the most technically sophisticated exploits we've ever seen," noting that it provided capabilities that were "previously thought to be accessible to only a handful of nation states."

SHOOTING THE MESSENGERS

Over the past decade, the rise of authoritarian regimes in many parts of the world has raised new questions about the durability of the liberal international order. As has been widely noted, many ruling elites have been able to slide toward authoritarianism by limiting or controlling political dissent, the media, the courts, and other institutions of civil society. Yet far less attention has been paid to the pervasive role of the mercenary spyware industry in this process. This neglect is partly the result of how little we know about spyware, including, in many cases, the identity of the specific government agencies that are using it. (Given the secretive nature of spyware transactions, it is far easier to identify victims than operators.) There is little doubt, however, that spyware has been used to systematically degrade liberal democratic practices and institutions.

One of the technology's most frequent uses has been to infiltrate opposition movements, particularly in the run-up to elections. Researchers have identified cases in which opposition figures have been targeted, not only in authoritarian states such as Saudi Arabia and the UAE but also in democratic countries such as India and Poland. Indeed, one of the most egregious cases arose in Spain, a parliamentary democracy and European Union member. Between 2017 and 2020, the Citizen Lab discovered, Pegasus was used to eavesdrop on a large cross section of Catalan civil society and government. The targets included every Catalan member of the European Parliament who supported independence for Catalonia, every Catalan president since 2010, and many members of Catalan legislative bodies, including multiple presidents of the Catalan parliament. Notably, some of the targeting took place amid sensitive negotiations between the Catalan and Spanish governments over the fate of Catalan independence supporters who were either imprisoned or in exile. After the findings drew international attention, Paz Esteban, the head of Spain's National Intelligence Center, acknowledged to Spanish lawmakers that spyware had been used against some Catalan politicians, and Esteban was subsequently fired. But it is still unclear which government agency was responsible, and which laws, if any, were used to justify such an extensive domestic spying operation.

In some countries, spyware has proved equally effective against journalists who are investigating those in power, with far-reaching consequences for both the targets and their sources. In 2015, several devices belonging to Mexican journalist Carmen Aristegui and a member of her family were sent Pegasus exploit links while she was investigating corruption involving then Mexican President Enrique Peña Nieto. There is no smoking gun that identifies the responsible party, though strong circumstantial evidence suggests a Mexican government agency. In 2021, a Hungarian journalist investigating corruption in President Viktor Orban's inner circle was hacked with Pegasus. (The Hungarian government subsequently acknowledged that it had purchased the technology.) And that same year, the cellphone of *New York Times* Middle East correspondent Ben Hubbard was infected with Pegasus while he was working on a book about Saudi Arabia's de facto leader, Crown Prince Mohammed bin Salman.

One Egyptian opposition leader was targeted by two different governments.

Almost as frequently, spyware has been used to undermine judicial officials and civil society organizations that are trying to hold governments to account. Take the case of Alberto Nisman, a well-known Argentine anticorruption prosecutor who was investigating an alleged criminal conspiracy by high-level Argentine officials. In January 2015, Nisman was found dead in suspicious circumstances—his death was later ruled a homicide—the day before he was to provide testimony to Congress implicating then president of Argentina Cristina Fernández de Kirchner and her foreign minister, Héctor Timerman, in a cover-up of alleged Iranian involvement in the 1994 bombing of a Jewish center in Buenos Aires. Later that year, the Citizen Lab documented how a South American hack-for-hire group had been contracted to target Nisman with spyware before his death, suggesting that someone in power was keen to peer into his investigations. In Mexico in 2017, a still unknown government agency or agencies used Pegasus spyware against human rights groups and international investigators that were tracking down potential government cover-ups of the notorious disappearance and gruesome murder of 43 students in Iguala, Mexico. Subsequent reports showed that the Mexican government had badly botched the investigations and that government personnel were implicated in a cover-up—findings that might never have come to light without the efforts of civil society watchdogs.

Other common Pegasus targets are lawyers involved with prominent or politically sensitive cases. In most liberal democracies, attorney-client privilege is sacrosanct. Yet the Citizen Lab has identified a variety of cases in which spyware has been used to hack or target lawyers' devices. In 2015, the tactic was used against two lawyers in Mexico who were representing the families of Nadia Vera, a slain government critic and women's rights advocate. More recently, multiple lawyers representing prominent Catalans were targeted as part of the Spanish surveillance campaign. And in Poland, Pegasus spyware was used several times to hack the device of Roman Giertych, legal counsel to Donald Tusk, a former prime minister and the leader of the country's main opposition party. (In early 2022, Polish Deputy Prime Minister Jaroslaw Kaczynski publicly acknowledged that the government had bought Pegasus spyware but denied that it had been used against the Polish opposition.)

As the availability of spyware grows, private-sector clients are also getting in on the act. Consider the activities of BellTroX, an Indian hack-for-hire company responsible for extensive espionage on behalf of private clients worldwide. Between 2015 and 2017, someone used BellTroX's services against American nonprofits that were working to publicize revelations that the oil company ExxonMobil had hidden its research about climate change for decades. BellTroX has also been used to target U.S. organizations working on net neutrality, presumably at the behest of a different client or clients that were opposed to that reform. BellTroX also has a burgeoning business in the legal world; law firms in many countries have used the company's services to spy on opposing counsel. In April 2022, an Israeli private detective who acted as a broker for BellTroX pleaded guilty in U.S. court to wire fraud, conspiracy to commit hacking, and aggravated identity theft, but BellTroX's India-based operators have remained out of reach of the law. (Asked by Reuters in 2020 to respond to the findings, the company's founder, Sumit Gupta, denied any wrongdoing and declined to disclose his clients.)

NOWHERE TO HIDE

The proliferating use of spyware against political and civil society targets in advanced democracies is concerning enough. Even more threatening, however, may be the ways in which the technology has allowed authoritarian regimes to extend their repression far beyond

their own borders. In past decades, autocrats faced significant barriers to repressing citizens who had gone into exile. With spyware, however, an operator can get inside a political exile's entire network without setting foot inside the target's adopted country, and with very few of the risks and costs associated with conventional international espionage.

Examples of this new form of transnational repression are manifold. Beginning in 2016, Cyberbit was used to target Ethiopian dissidents, lawyers, students, and others in nearly 20 countries. In 2021, the phones of two prominent Egyptians—exiled opposition politician Ayman Nour, who has been living in Turkey, and the host of a popular news program (who has asked to remain anonymous for his own safety)—were hacked with Cytrox's Predator spyware. In fact, the phone of Nour, who is an outspoken critic of Egyptian President Abdel Fattah el-Sisi, was simultaneously infected with both Predator and NSO Group's Pegasus spyware, each apparently operated by separate government clients—Egypt in the case of Predator and either Saudi Arabia or the UAE in the case of Pegasus. In a statement to *Vice News,* Cyberbit said that the Israeli government oversees its technology and that "the intelligence and defense agencies that purchase these products are obligated to use them in accordance with the law." In the Egyptian hacking case, Cytrox's CEO, Ivo Malinkovski, declined to comment; according to VICE news, he subsequently deleted references to Cytrox in his LinkedIn profile. (The governments of Egypt, Ethiopia, Saudi Arabia, and the UAE have declined to comment about the findings.)

Especially far-reaching has been the Saudi government's transnational spyware campaign. In 2018, a phone belonging to Ghanem al-Masarir, a Saudi dissident living in the United Kingdom, was hacked with Pegasus spyware. Coinciding with the infection of his device, al-Masarir was tracked down and physically assaulted by Saudi agents in London. Spyware may have also played a part in the notorious killing of the exiled Saudi journalist Jamal Khashoggi in the Saudi consulate in Turkey. In 2018, a phone owned by Omar Abdulaziz—a Saudi activist, Canadian permanent resident, and close confidant of Khashoggi—was hacked with Pegasus spyware. Abdulaziz and Khashoggi had been discussing their activism against the Saudi regime over what they mistakenly assumed were secure communications platforms. After Khashoggi's killing, forensic analysis revealed that the devices of several other people closest to Khashoggi, including his Egyptian wife and his Turkish fiancée, had also been infected. To what extent Khashoggi's own phones were hacked is not known because his fiancée turned them over to Turkish authorities, who have withheld them from independent analysis, but his closest contacts were all under surveillance, providing Saudi agents with windows into Khashoggi's personal life, political activism, and movements in the months leading up to his murder. (The Saudi government has declined to comment on the revelations. In 2021, NSO Group told *The Guardian*, "Our technology was not associated in any way with the heinous murder of Jamal Khashoggi.")

One exploit can turn on a user's microphone and camera.

In fact, targeting regime critics abroad with spyware is only one of several ways the Saudi government has employed digital technology to neutralize dissent. For example, according to a U.S. federal indictment, a top adviser to Saudi Crown Prince Mohammed bin Salman paid a Twitter employee $300,000 and provided other gifts in 2014 and 2015, apparently in exchange for spying on dissidents on the platform. The employee, who left Twitter in 2015, was convicted in U.S. court in 2022. When such tactics are used in combination with the type of highly intrusive surveillance that spyware represents, dissidents can come under extraordinary psychological pressure. Many victims of hacking have experienced debilitating shock knowing that their compromised devices have also put friends and associates at risk and that their every move is being watched. One female Saudi activist explained that being digitally targeted was a form of "psychological and emotional war" that caused her "endless fear and anxiety." By using spyware, autocrats and despots are thus able to clamp down on civil society networks well beyond their own borders even as they strengthen autocracy at home.

Despite a large and growing body of documentation about spyware abuses around the world, there are several reasons that the technology seems likely to become even more widespread. First, although much scrutiny of mercenary spyware firms has concerned their contracts with national government agencies, many firms market to more than one client in a given country, including local law enforcement. For example, in a fact-finding trip to Israel in the summer of 2022, officials for the European Parliament learned that NSO Group has at least 22 clients in 12 European countries, suggesting that a significant number of these clients are subnational agencies. Such deals raise further questions about accountability, given that research has shown that local law enforcement agencies are often more susceptible to abuses, such as racial profiling or corruption, and tend to have poor transparency and insufficient oversight.

Second, although some mercenary spyware firms such as NSO Group claim that they deal only with government clients, there is little to prevent them from selling their technology to private firms or corrupt individuals. Evidence suggests that some already do: in July 2022, Microsoft's Threat Intelligence Center issued a report on an Austria-based spyware and hack-for-hire firm called DSIRF that had targeted individuals in banks, law firms, and consultancies in several countries. Though Microsoft did not specify what type of clients hired DSIRF, the firm advertises "due diligence" services to businesses, implying that these hacking operations were undertaken on behalf of private clients. When Reuters asked DSIRF about the Microsoft report, the company declined to comment. Although it is illegal if done without a warrant, such private-sector hacking is less likely to be deterred when hackers' firms are located outside the jurisdiction in which the targeting occurs. As protections for privacy rights, freedom of the press, and independent courts, come increasingly under threat in many countries, it will likely become even easier for corrupt firms or oligarchs to deploy mercenary spyware without accountability.

Third, spyware has become a central component of a broader menu of surveillance tools, such as location tracking and biometric identification, used by many government security agencies. The more that spyware is incorporated into everyday intelligence gathering and policing, the harder it will be to rein it in. More ominously, spyware may soon acquire even more invasive capabilities by exploiting wearable applications, such as biomedical monitors, emotional detection technology, and Internet-connected neural networks currently in development. Already, many digital applications aim to drill deeper into the subliminal or the unconscious aspects of users' behavior and gather data on their health and physiology. It is no longer science fiction to envision spyware that might use covert access to these data about our biological or cognitive systems to monitor and even manipulate a victim's behavior and overall well-being.

RESTRAINING ORDERS

For nearly a decade, the mercenary spyware industry has been able to expand its reach across the globe largely without regulation or accountability. But that is a choice governments have made, not an inevitable outcome that must simply be accepted. As civil society watchdogs and journalists have brought to light flagrant abuses, it has become more difficult for major spyware vendors and government clients to hide their operations. In Europe and the United States, committees have held hearings on spyware, and government agencies have begun to develop new policies to limit its use. Notably, the U.S. Commerce Department has placed NSO Group, Candiru, and other hack-for-hire firms on an export restriction list, limiting their access to U.S. products and technology and sending a strong signal to potential investors that spyware companies are under growing scrutiny. Technology platforms have also taken action. Meta (the parent company of Facebook) and Apple have sued NSO Group in U.S. courts, notified victims of spyware infections, and worked to support civil society watchdogs. Apple has also donated $10 million to cybersurveillance research and has pledged to do likewise with any damages awarded from its lawsuit against NSO Group.

But curbing the global spread of mercenary spyware will require a comprehensive approach. To begin with, companies need to devote far more resources to identifying and rooting out spyware and ensuring that their services are properly secured against exploitation. WhatsApp and Apple have already shown how to alert victims when spyware is detected and hold spyware vendors such as NSO Group legally responsible for violations of their terms of service and other legal offenses. Whether through a shift in business culture, or more likely through stronger government regulations, technology platforms should also put more emphasis on security and scale back the relentless quest to vacuum up user data. In turn, the forensic investigations of the Citizen Lab, Amnesty International, journalists, and others will need to be broadened and supplemented by other organizations doing similar work, whether at NGOs, universities, or investigative news organizations. Digital forensic science and digital accountability should be recognized as a formal research discipline that can monitor spyware activity, assist victims and targets, and keep pressure on governments and corporations to be more transparent and accountable for their actions. For such a field to emerge, many years of public, private, and philanthropic support will be needed.

Ultimately, governments themselves will need to adopt a robust regulatory framework for spyware use. Regulating the industry will likely require the enactment of a complex set of rules that address various aspects of the spyware market. For example, domestic-based spyware companies could be required to make regular public disclosures about their exports, and, in turn, government agencies could be required to report from whom and where they are importing spyware. Export rules need to be strengthened to prevent the sale of spyware to governments or other clients that are likely to use them in violation of international human rights law. Clear rules and standards of oversight for the use of spyware are also necessary. Specific legislation addressing the zero-day market will likely also be needed, although it will have to be carefully crafted so that legitimate security research is not hindered. Governments could also pass legislation giving victims of spyware the right to sue both foreign governments and spyware vendors for harms caused by espionage.

Such efforts could be reinforced at an international level through the development of a global spyware control regime. Military activities, for example, have long been subject to international oversight through such mechanisms as the UN's Register of Conventional Arms and the policies that have been put in place relating to standards for private military and security contractors or the banning of land mines. A similar process could lead to the international regulation of spyware, including requirements for transparency and reporting about its use. These existing models, however, suggest that success will require the buy-in of a significant number of countries, and more pressure is needed to persuade governments and world leaders that mercenary spyware poses a serious and growing threat to international security and the liberal international order.

No doubt, authoritarian governments and security agencies that currently benefit from spyware will seek to obstruct such regulation, but the growing risks to national security of an unregulated market may prompt a more sober assessment. In November 2022, Sir Jeremy Fleming, a top British intelligence official, warned that the proliferating use of mercenary spyware and "hackers for hire" by countries and malefactors "will increase the future threat to UK cybersecurity." Should the use of mercenary spyware continue to grow unchecked, the risks for democracy will become acute. If elites in any country can use this technology to neutralize legitimate political opposition on any point on earth, silence dissent through targeted espionage, undermine independent journalism, and erode public accountability with impunity, then the values on which the liberal international order is built may soon be no more secure than the passwords on our phones.