Written testimony of John Scott-Railton, Senior Researcher, the Citizen Lab
House Permanent Select Committee on Intelligence
Hearing on "Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware"

July 27, 2022

Chairman Schiff, Ranking Member Turner, and esteemed Members of the Committee:

Thank you for this opportunity to testify today, and for your continuing efforts to address the many serious threats posed by the mercenary spyware industry.

My name is John Scott-Railton. I am a Senior Researcher at the Citizen Lab, a research group based at the University of Toronto's Munk School School of Global Affairs & Public Policy. We do independent academic research into digital threats, focusing on attacks against civil society, censorship, and disinformation.

The Citizen Lab's mandate is concerned with how these threats impact civil society, whether nonprofits, journalists, human rights defenders, and more. We are transparent about our funding, strictly independent of both corporations and governments, and never undertake commissioned research.[1]

Our research includes working closely with high-risk civil society groups around the world, and examining and publishing on the digital threats they face. For the past decade, a growing fraction of the cases that we have encountered involve mercenary spyware.

This testimony is developed from a body of evidence assembled by my colleagues and peers, and a field of talented researchers in academia, industry, and non-profit organizations. Many more groups have helped with victim outreach, collecting cases, and collaborating in investigations. Investigative journalists and reporting collectives have also played a significant role in shedding light on this secretive world. I cannot speak for anyone else in this growing ecosystem of accountability, but without their critical work, this conversation would not be happening. I would also like to acknowledge the colleagues that helped me prepare this testimony, as well as Dr. Bill Marczak, whose work developing techniques for scanning for various mercenary spyware families has led to many of our recent discoveries.

It is also very meaningful to me that Carine Kanimba has been invited to testify. As a victim of Pegasus spyware, she will be able to tell you about the impact of being targeted during her efforts to secure the release of her father, Paul Rusesabagina, from jail in Rwanda. Much of what we know about mercenary spyware abuses come from brave victims stepping forward, despite the risks. We owe them a great debt.

[1] The Citizen Lab, "About," *The Citizen Lab*, https://citizenlab.ca/about/.

Part 1: Proliferating Capabilities For Sophisticated Hacking

Less than twenty years ago, only a relatively small set of states could engage in sophisticated, invisible-to-the-target, hacking of phones and computers at nearly any scale. As a shorthand, I call these Tier A states. They typically have a robust STEM pipeline (e.g., access to PhD students in cryptography and computer science). These states may also have domestic offensive developers that exclusively supply to them, or to a handful of allies such as the Five Eyes. This group includes the U.S., France, U.K., Israel, Russia, China, Australia, and so on.

Even as a growing list of governments around the world are busily working to develop their own endogenous capabilities, a new tier has emerged: **pay-to-play government customers**.

While the pay-to-play tier may lack a robust STEM pipeline, they do have checkbooks. They are supplied by the **mercenary spyware industry**, which sells an increasingly sophisticated set of espionage capabilities to a growing global customer list.[2]

In many cases, the talent pool of mercenary spyware developers draws from veterans of the intelligence services of U.S. allies. This includes countries with whom the U.S. has intelligence-sharing relationships.

While some pay-to-play customers are situated within governments with a degree of oversight, many are operating without any clear oversight or accountability. Predictably, this ballooning customer list is responsible for many of the abuses that have been uncovered.

How 'Good' is Mercenary Spyware Technology?

The U.S. Government has extensive offensive capabilities against phones and computers. While the mercenary spyware industry probably cannot match them, some companies are getting closer. The growing use of "zero-click" exploits is illustrative.

"Zero-click," which refers to exploits that do not require any victim interaction, means that operators no longer need to rely on tricking victims into clicking links or opening files in order to infect their device.

The risk does not come from sitting in a cafe and connecting to unsecured Wi-Fi. Your phone can be on your bedside table at 2 a.m., and the spyware operator a continent away. One moment the device is clean. The next? Your data is silently streaming to an adversary.

Google's Project Zero recently described a zero-click exploit used by NSO Group, which they identified based on forensic artifacts that we shared with them, as:

---

[2] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert (2018), "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab*, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

> *"...one of the most technically sophisticated exploits we've ever seen, further demonstrating that the capabilities NSO provides rival those previously thought to be accessible to only a handful of nation states."*[3]

Unfortunately, there are few, if any, actions available to phone users to protect themselves from zero-click exploits. Even U.S. officials are not immune.

What Can Mercenary Spyware Do On An Infected Device?

The most notorious mercenary spyware currently available is NSO Group's Pegasus, although there are many others. Pegasus' capabilities on an infected phone broadly match many other mercenary spyware products. With Pegasus, the user can access the following, and more, on an infected device:[4]

- Your texts and calls
- Your encrypted texts, like those in WhatsApp and Signal
- Your pictures and notes
- Your contacts, emails, etc.

In short, Pegasus can do anything on your phone that you can do. And some things you can't, like:

- Silently enabling the microphone or the camera and turning your phone into a bug in your pocket.
- Stealing the tokens that your phone uses to access cloud accounts, potentially enabling the attacker to maintain access to accounts long after an infection is over.[5]

This kind of mercenary spyware is highly sophisticated, invasive, and difficult to detect at scale, even by well-resourced governments.

---

[3] Ian Beer and Samuel Groß (2021), "A Deep Dive into an NSO Zero-Click iMessage Exploit: Remote Code Execution," *Google Project Zero*, https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html.

[4] Bill Marczak and John Scott-Railton (2016), "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender," *The Citizen Lab*, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

[5] Mehul Srivastava and Tim Bradshaw (2019), " Israeli Group's Spyware 'Offers Keys to Big Tech's Cloud,'" *Financial TImes,* https://www.ft.com/content/95b91412-a946-11e9-b6ee-3cdf3174eb89.

Part 2: Harms to National Security, Foreign Policy, and Human Rights

As the number of pay-to-play government operators continues to grow, we have seen an avalanche of abusive targeting. In these cases, the hacking is often clearly in breach of international human rights law and contrary to democratic values.

However, in response to what has become a drumbeat of reported abuses, the mercenary spyware industry typically claims that they are merely aberrations, and that the technology is designed *only* to combat crime and terror.

The facts do not bear this out in two ways.

First, we know from a decade of discoveries that **abuses are a persistent feature of any hacking technology when sold widely**. This was true a decade ago with companies like Gamma Group[6] (which made FinFisher), and Hacking Team.[7] It is still true today.

Secondly, the 'crime and terror' narrative omits the fact that a **substantial fraction of the targeting is espionage**.

In fact, some mercenary spyware customers seem to use the technology primarily to spy on other governments' officials. We know this not only from reporting like the Pegasus Project,[8] which was led by Amnesty International and Forbidden Stories, but also because, when we at Citizen Lab have reviewed samples of all targeting using a particular exploit from a particular period of time, a substantial fraction of that targeting appears to be states targeting each other.

The mercenary spyware industry knows that expanding espionage capabilities is a core part of their business model. But, it is inconvenient for them to acknowledge, as this quickly leads to the critical question: when does the industry become a threat to the U.S. national security and counterintelligence?

The answer: it already has.

---

[6] ECCHR (2022), "Criminal Complaint against Illegal Export of Surveillance Software is Making an Impact," *ECCHR*, https://www.ecchr.eu/en/press-release/criminal-complaint-against-illegal-export-of-surveillance-software-is-making-an-impact/.

[7] Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton (2014), "Mapping Hacking Team's 'Untraceable' Spyware," *The Citizen Lab,* https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/.

[8] The Guardian, "The Pegasus Project," *The Guardian*, https://www.theguardian.com/news/series/pegasus-project.

Turbocharging Counterintelligence Threats

U.S. government personnel are not well-protected from mercenary spyware. The fact that some mercenary spyware companies claim that they prevent targeting people located in the U.S., or with U.S. phone numbers, does not address the threat posed by companies with no such restrictions. Nor does it address the fact that many U.S. officials working overseas must use phones with non-U.S. numbers.

Reportedly, at least nine U.S. officials were hacked with Pegasus spyware last year. Remarkably, this appears to have remained undetected until Apple made the discovery while investigating the FORCEDENTRY[9] zero click exploit used by NSO Group.[10]

Threats to U.S. officials from mercenary spyware are not new. Indeed, nearly a decade ago, when the industry was in its infancy, U.S. diplomats in Panama were already reportedly being targeted. This alleged incident was described in a motion supporting an extradition request between the U.S. and Panama.[11] The motion also reported allegations made by a witness that Panama's then-President would direct an associate to publish stolen audio of his rivals' private conversations on YouTube.[12]

I believe that these cases are only the tip of the iceberg. There is tremendous incentive for countries around the world to hack U.S. officials. Given past experiences, it is plausible that some cases have never been uncovered.

Recently, the Biden Administration recognized this threat when it added a number of mercenary spyware companies, including Candiru and NSO Group, to the Entity List. It also highlighted the human rights impact of the spyware industry.[13]

The U.S. is not alone in recognizing the risk posed by mercenary spyware. The European Union Agency for Cybersecurity (ENISA) has also recently listed mercenary hacking as a major risk.[14]

---

[9] Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert (2021), "FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild," *The Citizen Lab,* https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/.

[10] Christopher Bing and Joseph Menn (2021), "U.S. State Department Phones Hacked with Israeli Company Spyware - sources," *Reuters,* https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/

[11] E.g., Benjamin G. Greenberg, Acting United States Attorney (2017), Memorandum of Law in Support of Extradition, *United States District Court for the Southern District of Florida*, *Case No.: 17-22197-MC-UNA*, https://images.law.com/contrib/content/uploads/sites/292/2017/08/Martinelli-motion.pdf.

[12] Id.

[13] US Department of Commerce (2021), "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities," *US Department of Commerce*, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

[14] ENISA (2021), "ENISA Threat Landscape 2021," *ENISA*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

Hacks using mercenary spyware have also impacted some very close allies. In the past two years, for example, we have repeatedly notified the U.K. government of multiple Pegasus compromises in their Foreign Office by several *distinct governmental operators*, and even of a Pegasus infection within the networks of Number 10 Downing Street.[15]

Reporting by the Pegasus Project, meanwhile, suggests that globally at least ten prime ministers, three presidents, and even a king may have been selected for Pegasus targeting.[16]

Pegasus in Politics, Elections and Human Rights Abuses

The volume and variety of mercenary spyware abuses uncovered by different research groups, antivirus and threat intelligence companies, and platforms, is so extensive that it is difficult to summarize concisely. Let me illustrate by highlighting some of our recent findings.

Just last week, as part of a collaborative investigation, we confirmed evidence of Pegasus infections on the phones of activists and opposition politicians in Thailand.[17] Earlier this spring, we confirmed the targeting and hacking of Catalan politicians, including Members of the European Parliament.[18] Before that? Journalists in El Salvador,[19] Polish opposition politicians,[20] and Christian religious leaders in Africa[21]–just to cite a few examples from recent years.

---

[15] Ron Deibert (2022), "UK Government Officials Infected with Pegasus," *The Citizen Lab*, https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/.

[16] Craig Timberg, Michael Birnbaum, Drew Harwell and Dan Sabbagh (2021), "On the List: Ten Prime Ministers, Three Presidents and a King," *The Washington Post*, https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/.

[17] John Scott-Railton, Bill Marczak, Irene Poetranto, Bahr Abdul Razzak, Sutawan Chanprasert, and Ron Deibert (2021), *The Citizen Lab*, https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/

[18] John Scott-Railton, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, and Ron Deibert (2022), "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru," *The Citizen Lab,* https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/.

[19] John Scott-Railton, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Al-Jizawi, Salvatore Solimano, and Ron Deibert (2022), "Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware," *The Citizen Lab,* https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/.

[20] Vanessa Gera and Frank Baja (2021), "AP Exclusive: Polish Opposition Senator Hacked with Spyware," *AP News*, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab; Vanessa Gera and Frank Baja (2021), "AP Exclusive: Polish Opposition Duo Hacked with NSO Spyware," *AP News*, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e.

[21] John Scott-Railton, Siena Anstis, Sharly Chan, Bill Marczak, and Ron Deibert (2020), "Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware," https://citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo/.

Let's take the case of Senator Kryzstof Brejza. In 2019, he was hacked at least 33 times while managing the electoral campaign for the opposition in Poland. The hacking timeframe often tracked consequential events and meetings in the run-up to the election. At one point, messages reportedly stolen from his phone were also published in an attempt to discredit him.[22]

Of course, political spying, and hacking during elections, are nothing new. But tools like Pegasus make this easier, much more invasive, and very difficult to uncover.

Physical Distance is No Protection

Many mercenary spyware operators do not restrict themselves to hacking within their borders. Spyware like Pegasus has enabled them to conduct hacking thousands of miles away.

Spyware has long been a core part of the transnational repression toolkit used by dictatorships like China.[23] Now, a growing number of other states have gotten in on the action.

Washington, D.C. is a vibrant city. It is also home to many diaspora populations. Unsurprisingly, autocrats back home want to monitor them. Now, with the aid of mercenary spyware, they no longer have to dodge FBI counterintelligence to do so.

Just across the river in Virginia, for example, U.S.-based Ethiopian journalists were targeted with mercenary spyware sold by Hacking Team, a since-rebranded Italian mercenary spyware company.

Proliferation May be Fueling Non-State Access to Sophisticated Spyware

We have encountered troubling cases that speak to the possibility that non-state actors may be accessing or directing the use of mercenary spyware.

For example, in Mexico, a government health researcher, a consumer advocate, and an anti-obesity campaigner were all targeted with Pegasus. Why? They had all been actively campaigning for an increase in the tax rate on soda. Circumstantial evidence led us to speculate that their targeting might have been directed or requested by someone with a financial interest in soft drinks.[24]

---

[22] Vanessa Gera and Frank Baja (2021), "AP Exclusive: Polish Opposition Senator Hacked with Spyware," *AP News*, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab.

[23] The Citizen Lab (2014) Communities @ Risk: Targeted Digital Threats Against Civil Society, https://targetedthreats.net/

[24] John Scott-Railton, Bill Marczak, Claudio Guarnieri, and Masashi Crete-Nishihata (2017), "Bitter Sweet: Supporter of Mexico's Soda Tax Targeted With NSO Exploit Links," *The Citizen Lab*, https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/.

Meanwhile, in Mexico, we are already witnessing a troubling nexus between targeting and cartel activities. We documented the targeting of Javier Valdez, a journalist who wrote about drug trafficking and crime in Mexico and who was killed in a cartel slaying. Both Valdez's colleagues[25] and wife[26] were infected shortly after the hit. Meanwhile, the phone number of Mexican journalist Cecilio Pineda Birto was selected for possible targeting with Pegasus by a Mexican Pegasus client in the weeks prior to his killing by cartel hitmen.[27]

Other troubling reports from Mexico further suggest that spyware may be ending up in the hands of cartels.[28]

As the mercenary spyware business grows, there will be an inevitable focus on pushing the technology to subnational entities, such as regional police services. These groups can be expected to have an even lower ability to ensure adequate oversight, or control access to the technology.

Meanwhile, at least one NSO Group employee stole source code.[29] Another used the technology to target a love interest.[30] As the number of pay-to-play mercenary spyware customers grows, I believe it to be almost inevitable that the exploit code and technology may leak in ways that cause serious, large-scale harm.

In addition, while some of the more notorious mercenary spyware companies *do* appear to limit sales exclusively to governments, other players in the industry may also seek lucrative engagements with private individuals and companies. This possibility highlights the need for action.

---

[25] John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert (2018), "Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague," *The Citizen Lab,* https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/.

[26] John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert (2019), "Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware," *The Citizen Lab*, https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/.

[27] Nina Lakhani (2021) "Revealed: murdered journalist's number selected by Mexican NSO client," *The Guardian,* *https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto*

[28] Cecile Schilis-Gallego and Nina Lakhani (2020), "'It's a Free-for-All': How Hi-Tech Spyware Ends Up in the Hands of Mexico's Cartels," *The Guardian,* https://www.theguardian.com/world/2020/dec/07/mexico-cartels-drugs-spying-corruption.

[29] Charlie Osborne (2018), "Former NSO Employee Steals, Flogs Pegasus Mobile Hacking Tool for $50 Million," *ZDNet*, https://www.zdnet.com/article/former-nso-employee-steals-flogs-phone-hacking-tools-for-50-million/

[30] Joseph Cox (2020), "NSO Employee Abused Phone Hacking Tech to Target a Love Interest," *Vice*, https://www.vice.com/en/article/bvgwzw/nso-group-employee-abused-pegasus-target-love-interest.

Part 3: A Critical Moment, and an Opportunity for Action

It has taken us many years to get to this public conversation about the threats of mercenary spyware. But the conversation now needs to move at the pace of the proliferation. We cannot put this technology back into the box. But, we can and must slow proliferation.

U.S. Investments: A Key Target in Curbing the Mercenary Spyware Industry

One of the core impacts of the U.S. government's recent actions around mercenary spyware– namely, adding NSO Group and Candiru to the Entity List– has been to cool investment and acquisition interest.

But, if NSO Group goes bankrupt tomorrow, there are other companies, perhaps seeded with U.S. venture capital, that will attempt to step in to fill the gap. As long as U.S. investors see the mercenary spyware industry as a growth market, the U.S. financial sector is poised to turbocharge the problem and set fire to our collective cybersecurity and privacy.

Instead, investors must feel that they stand to lose on these deals. The Biden Administration sent that signal about NSO Group. Congress has the power to send that signal about *all* unaccountable players within the industry.

Areas of Potential Action to Curb The Mercenary Spyware Threat

Here are several areas of action that have the potential to make a serious impact on mercenary spyware companies:

- Congress should direct the U.S. Intelligence Community to identify problematic mercenary spyware companies, and use all tools at their disposal to counter and disrupt their activities.
- Federal agencies should be prevented from doing business with identified problem companies. Getting federal contracts is the ultimate prize for any defense contractor, and their investors. Removing this opportunity would have an immediate impact.
- The U.S. should expand the tools available to hold identified problem companies, and their officers, accountable, including sanctions, and work to coordinate these actions with allies, such as the Five Eyes.
- The U.S. should apply diplomatic pressure to the countries that have become safe havens for the spyware industry, and that are enabling identified problem companies to thrive without regulation or oversight.

- Your committee put forward a sit-out period for operators from the intelligence community going to work for foreign offensive cyber operators.[31] This is a powerful disincentive. I encourage you to extend the timeframe from 30 months (and 5 years of reporting requirements) to a lifetime ban. We would not let a nuclear weapons scientist go work for a potential adversary in 3 years. We should not do so with hacking technology.
- Congress should develop legislation ensuring comprehensive U.S. export control and transparency requirements for domestically-developed spyware, including extensive due diligence for national security risks and human rights concerns.[32]
- The U.S. Government should continue to support internet security and privacy promoting technologies through the Open Technology Fund.

[31] US Senate Select Committee on Intelligence (2022), “Consolidated Appropriations Act, 2022,” *US Senate Select Committee on Intelligence*, https://www.intelligence.senate.gov/legislation/intelligence-authorization-act-fiscal-year-2022-division-x-consolidated-appropriations.

[32] US Department of State (2020), “U.S. Department of State Guidance on Implementing the "UN Guiding Principles" for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities,” *US Department of State*, https://www.state.gov/key-topics-bureau-of-democracy-human-rights-and-labor/due-diligence-guidance/.

Special Note: How Mercenary Spyware is Licensed

One common confusion about mercenary spyware concerns how the technology is licensed to customers. Some companies may charge simply for the provision of spyware with an unlimited number of possible targets. Others may charge by total number of targets in a given period. We believe that Pegasus is often sold with a number of 'licenses.' In this context, this specifies the number of *simultaneous infections*. For example, purchasing ten licenses authorizes a customer to have ten devices under monitoring at any given time. Analysis of victims' devices suggests that it may be a common practice for customers to infect for fairly brief periods, enabling them to use the same set of licenses to monitor a much larger set of individuals over time. In this manner, a single governmental customer with only ten licenses might be able to infect hundreds or more individuals in a year.

The preference for re-infection over persistence can lead to startling numbers of unique infections. For example, a journalist investigating the relationship between El Salvador's president and organized gangs was hacked on more than forty occasions.[33] During the times that his phone was *not* infected, we can assume that the licenses were being used to infect others' phones.

[33] John Scott-Railton, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Al-Jizawi, Salvatore Solimano, and Ron Deibert (2022), "Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware," *The Citizen Lab,* https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/.