COMBATTING THE THREATS TO U.S. NATIONAL SECURITY

FROM THE PROLIFERATION OF FOREIGN COMMERCIAL SPYWARE

Wednesday, July 27, 2022

U.S. House of Representatives,

Permanent Select Committee on Intelligence,

Washington, D.C.

The committee met, pursuant to call, at 10:04 a.m., in Room 2322, Rayburn House Office Building, the Honorable Adam Schiff (chairman of the committee) presiding.

Present: Representatives Schiff, Himes, Carson, Speier, Quigley, Castro, Welch, Maloney, Demings, Krishnamoorthi, Cooper, Crow, Turner, Wenstrup, Crawford, Mullin, LaHood, Fitzpatrick, and Gallagher.

The Chairman. Good morning and welcome. The committee will come to order. Without objection, the chair may declare a recess at any time.

This session will be conducted entirely on an unclassified basis. All participants are reminded to please refrain from discussing any classified national security information protected from public disclosure.

Today we are convening a public hearing on the acute and rapidly evolving threat posed by foreign commercial spyware. Public reports have shined a bright light on the robust market for powerful spying tools that are sold on the open market, essentially offering sophisticated signals intelligence capabilities as an end-to-end service.

The most sophisticated of these tools provide zero-click access to all the information stored on a mobile phone, laptop, or other internet-connected device. Emails, photographs, messages sent via encrypted apps, even the microphone on a device, literally nothing is out of reach.

This spyware could be used against every member of this committee, every employee of the executive branch, every journalist or political activist, every American citizen, every citizen of the world with an electronic device.

And aside from periodically updating the software on our devices, there is little that you can do currently to protect yourself from being targeted and compromised.

The availability of these tools in the hands of governments who previously lacked robust surveillance capabilities is truly a game-changer for U.S. national security, which makes it an issue of particular concern to this committee.

It is also a game-changer for autocratic regimes that are looking for new means to surveil, intimidate, imprison, or even kill dissidents, journalists, and others who they view as a threat.

In 2021, a group of news organizations and researchers, acting under the banner of the Pegasus Project, sounded a public alarm about the potential for these hacking tools to be abused. Their starting point was a leaked list of more than 50,000 phone numbers

that had been targeted by governments using spyware sold by one company, NSO Group.

Since that disclosure, a steady stream of disturbing reports has revealed that thousands of journalists, civil society activists, and many others have had their devices compromised by NSO's tools.

One such individual, Carine Kanimba, is here with us today. She will share the consequences of being targeted with spyware and what that has meant for her family.

Ms. Kanimba's experience should serve as a stark warning of the future that awaits us if countries and the private sector do not ban together to act decisively to rein in foreign spyware companies.

But the threat is not limited to people only like Ms. Kanimba. It is also a threat to millions of Americans and others around the world, and particularly U.S. Government personnel serving overseas.

Late last year, multiple news organizations reported that mobile phones used by U.S. diplomats in Uganda had been compromised by NSO's Pegasus tool.

It is my belief that we are very likely looking at the tip of the iceberg, and that other U.S. Government personnel have had their devices compromised, whether by a nation-state using NSO's services or tools offered by one of its lesser-known but equally potent competitors.

The Biden administration has recognized the national security threat posed by commercial spyware and has taken action. Last November, the Commerce Department added four companies, including NSO Group, to its Entity List, which blocked them from accessing U.S. technology.

The Commerce Department stated this action was, quote, "based on evidence that these entities developed and supplied spyware to foreign governments," and that these companies' activities were, quote, "contrary to the national security or foreign

policy interests of the United States."

Unfortunately, these listings have not deterred NSO and other foreign spyware companies from selling their tools to countries that could otherwise never develop such sophisticated surveillance capabilities indigenously.

Clearly, additional actions are needed.

The Intelligence Authorization Act, which was voted out of the committee on a unanimous, bipartisan basis last week, provides the Director of National Intelligence and the President with additional tools to rein in spyware companies, and also to ensure that foreign governments that target American officials pay a heavy price.

Among the measures in our bill are sweeping new authorities for the DNI to prohibit the Intelligence Community from acquiring and using foreign spyware.

Our bipartisan legislation further authorizes the DNI to block Intelligence Community contracts with U.S. companies that acquire, in whole or in part, any foreign spyware tool.

We also granted the President new authority to sanction foreign spyware companies, their executives, and foreign government officials who target American officials with spyware.

The nature of these foreign spyware tools makes them exceptionally hard to track and combat, and that is precisely why the United States needs to put a greater emphasis on this threat, with the Intelligence Community playing a critical and leading role.

I look forward to the testimony today to assist this committee in making sure we respond to this threat with urgency.

And with that, I now recognize Ranking Member Turner for his opening statement.

[The statement of The Chairman follows:]

******** COMMITTEE INSERT ********

Mr. Turner. Thank you, Mr. Chairman.

I want to thank all of the witnesses today.

Ms. Kanimba, I want to thank you particularly for coming in and sharing your personal story and for the story of your family.

Today we will hear about the threats associated with foreign commercial spyware technology and how it has reportedly been used to target journalists, protesters, and advocates and others, including U.S. citizens.

Spyware is not a new threat. However, the foreign commercial spyware that we are discussing today is focused on the ability of nation-states and others to purchase a complete surveillance apparatus that they may abuse to target opponents and dissidents.

It is commonplace to hear about this level of authoritarian control related to China, Russia, North Korea, or Iran, but it is more shocking to read about abuses of this technology from democratic governments and others, even those that we consider allies.

There are also growing counterintelligence concerns related to the potential targeting of U.S. citizens.

Addressing these threats must involve a mix of government and industry action. The Biden administration has placed four companies on the Department of Commerce Entity List, and the White House has indicated plans to release an executive order further placing limits on this technology.

This committee has also passed legislation to increase Intelligence Community collection on this threat, limit the IC's procurement of commercial spyware, and enhance detection and mitigation efforts.

The private sector must also do more to detect these threats, address vulnerabilities in technology, and provide users with the tools to keep their data secure.

This is true whether the threat is coming from a criminal actor or enterprise in a basement or from a nation-state.

I look forward to hearing from the witnesses today on the impact of foreign commercial spyware and how more can be done to mitigate the threat.

Thank you, Mr. Chairman. I look forward to the witnesses' testimony. I yield the balance of my time.

[The statement of Mr. Turner follows:]

******** COMMITTEE INSERT ********

The Chairman. Thank you, Mr. Turner.

With that, we will proceed with brief opening statements in the following order. First, Mr. Scott-Railton, a senior researcher with Citizen Lab who has helped to advance the public's understanding of the pernicious threat posed by foreign spyware; then, Mr. Huntley, who leads Google's Threat Analysis Group; and finally, Ms. Kanimba, who has been targeted by spyware.

Mr. Scott-Railton, you are recognized for your opening remarks.

STATEMENTS OF JOHN SCOTT-RAILTON, SENIOR RESEARCHER, THE CITIZEN LAB; SHANE HUNTLEY, DIRECTOR, THREAT ANALYSIS GROUP, GOOGLE; AND CARINE KANIMBA, TARGET OF FOREIGN COMMERCIAL SPYWARE

STATEMENT OF JOHN SCOTT-RAILTON

Mr. Scott-Railton. Thank you very much.

Chairman Schiff, Ranking Member Turner, and esteemed members of the committee, thank you for the opportunity to testify this morning and for your continuing efforts to address the problem of mercenary spyware.

My name is John Scott-Railton. I am a senior researcher at the Citizen Lab based at the University of Toronto's Munk School of Global Affairs.

Our investigations into digital threats put us in close touch with high-risk groups, like journalists, activists, and dissidents around the world.

Today most of the cases that come to us involve mercenary spyware.

Once upon a time, only a small group of states had the capability to engage in sophisticated targeting of devices like mobile phones and computers.

But in the past decade, a new tier of operators has emerged. This is pay-to-play governments, supplied by mercenary spyware companies.

Google, as they will tell you, tracks over 30 such vendors. There may be hundreds of government customers around the world, but the true scale of both the base of companies and the customers is unknown.

While the big players in the mercenary spyware industry claim to sell only to governments, their actions suggest comfort with blurred lines.

Slide, please.

Here is a privately owned heavy machinery warehouse in a dusty industrial section of Accra, Ghana. A Pegasus system was allegedly installed here as part of an illegal effort to monitor the opposition in the run-up to the Presidential election.

The mercenary spyware industry is getting close to some of the more advanced capabilities available to the United States Government.

Take the zero-click exploits that are being incorporated into mercenary spyware. Zero-click means that the victim doesn't have to click or open a file or perform any other action in order to be infected.

This isn't about sitting in a cafe and connecting to unsecured WiFi. Your phone can be on your bedside table at 2 in the morning. One minute your phone is clean; the next minute the data is silently streaming to an adversary a continent away. You see nothing.

Google's Project Zero calls this kind of technology, one of the exploits that we share with them, "one of the most technically sophisticated exploits" they had ever seen and said that it was capabilities available only to a handful of nation-states.

Here is what mercenary spyware can do, taking the example of Pegasus. It can access your texts and phone calls. It can access your encrypted chats, your pictures, your voice notes. Anything you can do on your phone, Pegasus can do -- and some things you can't, like silently enabling the microphone and the camera or gaining access to your cloud accounts.

It is clear that the United States Government is not immune from the mercenary spyware threat. Reportedly, at least 11 U.S. officials were targeted with Pegasus in Uganda last year. This had remained undetected, apparently, until Apple contacted and made this discovery while investigating a zero-click exploit that we had shared with them.

The mercenary spyware industry has a track record of enabling the hacking of U.S. officials.

Slide, please.

For example, nearly a decade ago, in a case that has gotten little attention, U.S. diplomats in Panama were reportedly infected with mercenary spyware.

Some of America's closest allies, like the United Kingdom, have also been targeted. In fact, we found evidence of an infection within the networks of the Office of the Prime Minister at No. 10 Downing Street.

I believe that these cases are the tip of the iceberg and there are many more yet to be discovered.

Recently, the Biden administration recognized the threat from mercenary spyware to America's national security and foreign policy when it added several vendors to the Commerce Department's Entity List. This was progress. And when the administration announced the designation, they rightly noted human rights harms.

The proliferation has also fueled an avalanche of abuses that violate international human rights law and are contrary to democratic values.

Just last week, we confirmed Pegasus infections of activists and lawmakers in Thailand. Before that, Catalan civil society and lawmakers. Before that, journalists in El Salvador, Polish lawmakers targeted during elections, and Christian religious leaders in Africa, to name just a few examples.

Just yesterday, we learned that the head of a major political party in Greece was targeted with Predator, another piece of mercenary spyware.

Slide, please.

As mercenary spyware proliferates, it is inevitable that nonstate actors will eventually get their hands on these sophisticated capabilities and cause large-scale harm.

When the deployment in Ghana was taken down, Pegasus servers were reportedly hidden at a private location and were found during a police raid.

Just today, Microsoft announced in their testimony that they disrupted a mercenary spyware actor that also sells to private payers.

In Mexico, we also see a troubling nexus between cartel killings and spyware targeting. And that, of course, as I think you are aware, only scratches the surface.

Unfortunately, we cannot trust the vendors to protect their capabilities either. An NSO Group employee stole source code for personal gain. Another used the technology to target a love interest.

It has taken us too long to have this conversation, but I am glad to have it, and now we must make sure that it moves at the pace of proliferation.

It is too late to put the tech back into the bottle, and so we must take strong action now and pump the brakes on proliferation to protect our national security and our human rights.

Financial investments, including from pension funds in the United States, have supercharged this problem. But when the United States Government added NSO Group and another vendor to the Entity List, this sent a strong signal, which is pretty powerful, and it impacted both NSO Group's valuation and investor confidence.

Congress should send that signal to all unaccountable players within the industry. Congress should direct the Intelligence Community to identify and use all tools at their disposal to counter and disrupt problem companies.

Problem companies should be barred from business with Federal entities, and American companies should be blocked from acquiring them.

The U.S. must also expand the tools available to hold problem companies, and their officers and executives and owners, accountable and work to coordinate these

activities with allies.

Finally, the U.S. should apply diplomatic pressure to the countries that have become safe havens for these problematic companies.

And with that, I thank you for your time.

[The statement of Mr. Scott-Railton follows:]

******** COMMITTEE INSERT ********

The Chairman. Thank you very much.

Mr. Huntley.

STATEMENT OF SHANE HUNTLEY

Mr. Huntley. Chairman Schiff, Ranking Member Turner, and esteemed members of the committee, good morning. My name is Shane Huntley, and I am the director of Google's Threat Analysis Group, or TAG.

TAG is the team within Google whose mission it is to analyze and disrupt serious and targeted threats against Google and our users. These include government-backed actors, serious cybercrime, and disinformation threat actors.

TAG is only one part of Google's large investment in making the internet more secure. We work with many other teams within the company, including Project Zero, Android, and Chrome security, and we also work across the industry, civil society, and with government to keep users safe online.

Thank you very much for inviting me to appear before you today. I appreciate this opportunity to explain to the committee how the commercial spyware industry is unfortunately thriving, creating risk to Americans and internet users across the globe, and what we are seeing.

The business model of commercial spyware is to make money by providing comprehensive and sophisticated cyber espionage capabilities to foreign governments, including both the exploits to gain control of the device and also the spyware software itself which can collect all sorts of personal information.

While these vendors claim to vet their customers and usage carefully with the

promise that the work is used to counter criminals and terrorists, what we have observed in TAG is consistent with others' reporting -- that again and again these tools are found to be used by governments for purposes antithetical to democratic values, targeting dissidents, journalists, human rights workers, and political opponents.

NSO Group is the most prominent actor offering spyware and these services, and with others we have been working for years to counter this threat and mitigate the damage.

In 2017, Google's Android was the first mobile platform to warn users about NSO Group's Pegasus spyware. At the time, our Android team released research about the spyware that was used in a targeted attack against a small number of Android users.

We notified the users, remediated the compromise, and implemented controls across all of Android to ensure further users were not infected by this version.

Later, in 2019, we were able to quickly fix a vulnerability in Android that was discovered by examining some leaked marketing information from NSO.

In December 2021, our Project Zero team published research about the novel techniques used by NSO Group to compromise iMessage users.

As mentioned previously, this was a zero-click exploit, meaning that iPhone users could be compromised by receiving a malicious iMessage text without ever needing to click on a malicious link.

We assessed this to be one of the most technically sophisticated exploits we had ever seen, and the ability for an end user to protect themselves from such a threat is very minimal.

But NSO is certainly not the only actor in this space. TAG is actively tracking more than 30 vendors with various levels of sophistication and public exposure, selling exploits or surveillance capabilities to government-backed actors.

We have publicly taken action to discover and counter exploits and malware produced by Equus, Cytrox, Candiru, and RCS Labs, amongst others, and countering these threat actors is becoming a bigger part of our work.

In 2021, my team discovered nine zero-day vulnerabilities being used in the wild, and seven of those were originally developed by commercial surveillance vendors.

The proliferation of commercial hacking tools is making the internet less safe and threatening our digital society and national security.

In addition to our direct work to counter these threats, we also work to develop and deploy industry-leading security features and protections to protect our users across our products, which is detailed in my written testimony.

This includes specific programs targeted for high-risk users and sites, such as our Advanced Protection Program and Project Shield.

We appreciate the committee's focus on this issue, and we recommend the U.S. Intelligence Community prioritizes identifying and countering threats from foreign commercial surveillance vendors.

We believe it is time for government, industry, and civil society to come together more to change the incentive structure which has allowed these technologies to spread in secret.

We welcome the recent application of sanctions against NSO Group and Candiru, and we recommend the U.S. Government consider a full ban on Federal procurement of commercial spyware technologies and contemplating proposing further sanctions to limit the spyware vendors' ability to operate in the U.S. and receive U.S. funding.

We also urge the United States to lead a diplomatic effort to work with the governments in countries who harbor these problematic vendors and also who employ these tools. And we need to build support for measures that limit harms by this

capability.

While we continue to fight these threats on a technical level, the providers of these capabilities operate openly in democratic countries and will continue to do so while the incentives make it in their interests.

Thank you for convening this important hearing. Google is committed to leading the industry in detecting and disrupting the threats posed by these commercial spyware, and I look forward to answering the committee's questions.

[The statement of Mr. Huntley follows:]

******** COMMITTEE INSERT ********

The Chairman. Thank you, Mr. Huntley.

Ms. Kanimba, you are now recognized for your opening remarks.

STATEMENT OF CARINE KANIMBA

Ms. Kanimba. Thank you.

Mr. Chairman, Ranking Member, members of the committee, thank you for welcoming me to speak with you today. My name is Carine Kanimba. I am the youngest of six children of Taciana and Paul Rusesabagina, and I am an American citizen.

The United States welcomed my family when we sought refuge, and we found safety and security within its borders.

I am a proud graduate of Northwestern University, and until 2 years ago I was working in a job I loved in finance based out of New York City.

In August of 2020, everything changed. Nearly 700 days ago, my father was lured from our family home in San Antonio, Texas, by an intelligence operation directed by the Rwandan Government.

He was kidnapped in Dubai and then illegally rendered to Kigali via private jet, chartered by the Office of the Rwandan President. He was tortured, subjected to a sham trial, and sentenced to 25 years in prison.

The United States Government has designated him as wrongfully detained, and the House has passed two resolutions already in support of my father and calling for his immediate release.

Our family is extremely grateful to the House and to Congressman Castro and Congresswoman Kim for leading the efforts of this resolution.

In 2021, I became the victim of NSO's Pegasus spyware.

I was born in Rwanda, just prior to the 1994 genocide that made me an orphan. My birth parents were among the first victims of nearly one million people killed during the genocide, leaving my sister, Anaise, and I orphans.

Anaise is a graduate of Georgetown University here in Washington, D.C., and she is here with me today.

My father, Paul Rusesabagina, is a hero of the genocide. In 1994, he was the manager of the hotel in Kigali, and he gave refuge to 1,268 people in his hotel, risking his life every single day to push back the militia that was waiting outside, and not a single person was killed.

Once the killings finally ended, my adoptive parents, Taciana and Paul, heard that our parents had been killed, and they searched for Anaise and I, found us in a refugee camp, raised us and loved us as their own, along with my new brothers and sisters, Lys, Roger, Dan, and Tresor.

My mother, Taciana, is here with us today.

In 2004, the story was portrayed in the film "Hotel Rwanda," and my father's name became known all over the world as a man of peace and virtue. In 2005, he was awarded the U.S. Presidential Medal of Freedom, the highest honor in our country.

My father was given a platform, and he used it for good. He was critical of the increasing violations of human rights of Rwandans, calling loudly for democracy, freedom of speech and press, as well as truth and reconciliation for all Rwandans.

This criticism turned him into a target of the Rwandan President, Paul Kagame. The campaign was targeted and brutal. Assassination attempts against my father's life in Belgium, house break-ins, and intimidation attempts.

But my father was never intimidated, because he knew that he had a

responsibility to use his platform to be the voice for the silent victims of the 30-year Rwandan dictatorship.

President Kagame has called my father's kidnapping a flawless operation. It was flawless because Rwanda surveilled and tracked him in San Antonio, Texas, and publicly boasted about doing so.

With the passage of the Robert Levinson Act of 2020, we hope that the new measures, like sanctions and denial of entry into the United States, will help prevent other American families from being targeted like us.

In February 2021, I was contacted by a collective of journalists called Forbidden Stories, working with Amnesty International and Citizen Lab on the Pegasus Project.

Their research on Rwanda and Pegasus gave them reasons to believe that I was being spied on. They asked to conduct forensics analysis on my phone, and I agreed.

It was then discovered that Pegasus surveillance had been used to target me. I was mortified and I am terrified.

The forensics reports have been presented to this committee, and they show that the spyware was triggered as I walked in with my mom into a meeting with the Belgian Minister of Foreign Affairs.

It was active during calls with the U.S. Presidential Envoy for Hostage Affairs team, and the U.S. State Department, as well as U.S. human rights groups.

This surveillance is illegal under U.S. law, and it allowed the Rwandan Government to stay a step ahead as we fought to keep our father alive.

I am told that my surveillance would cost the Rwandan Government millions of dollars. Rwanda is the third-most aid-dependent country in the world. Foreign aid makes up to 70 percent of national expenditure, and the U.S. provided $160 million in aid to Rwanda last year.

All of you, Members of Congress, and American taxpayers themselves, deserve to know how the Government of Rwanda is spending humanitarian aid.

Then, 2 months ago, Citizen Lab also discovered that my cousin Jean-Paul Nsonzerumpa's phone had been infected. Jean-Paul and I live in the same house. Now two phones in the same household being targeted by the same software, by the same repressive regime.

I am frightened by what the Rwandan Government will do to me and my family next. It keeps me awake that they knew everything I was doing, where I was, who I was speaking with, my private thoughts and actions, at any moment they wanted.

Unless there are consequences for countries and their enablers which abuse this technology, none of us are safe.

Thank you for letting me share my story and the story of my father, Paul Rusesabagina. I hope that you find it useful in considering how to regulate the type of tools used to target my family and my father.

I promise you all that we will not stop advocating for him until he is home.

Thank you.

[The statement of Ms. Kanimba follows:]

******** COMMITTEE INSERT ********

The Chairman. Thank you, Ms. Kanimba, for that very powerful testimony. Deeply regret what you have gone through, what your father is going through, what your whole family has experienced, and very much appreciate your willingness to come in and speak with us today.

I will now recognize myself as we begin the question period.

Let me start, Mr. Huntley, by asking about the zero-click exploits. How common are they? Do we have any idea? And is there anything that individual users, consumers, can do to protect themselves from these exploits?

Mr. Huntley. The discovery of these exploits is actually fairly rare, and it has maybe opened a debate about how common they are. We do believe they are very rare. As we said, this was one of the most sophisticated exploits we have ever seen, but the full scope of the problem is unclear.

One of the challenges with such sophisticated exploits is that there is no sign. So if it is being used in a limited way, then we do not have the visibility of what is happening.

We do believe that what users can do is actually also very limited as well.

Our approach inside Google very much is that we want to make it a lot harder to do these zero-day exploits.

When we say zero-day exploits, we mean these exploits where there is no patch available and no protection in the platform, so the user is vulnerable.

So when my team discovers a zero-day exploit in the wild, we give the manufacturer or ourselves 7 days to fix it, and we fix it very quickly. And that is the biggest protection we can do.

What we have to do is secure these platforms, find the exploits in use, find the exploits that aren't in use yet, and then continue to secure these platforms, because that

is the primary mechanism we have to protect users against these threats.

The zero-click exploit in this case, the analysis actually showed that it had been in use for months. So that means that over that period of months, NSO customers were able to silently target any iPhone user they wanted.

The Chairman. Because these don't require users to click on a link or be fooled by some spear phishing effort, it sounds like other than keeping your phone up to date, there is really nothing you can do to protect yourself.

Mr. Huntley. Against the zero-click side to it, it is very limited what you can do, yes.

I would say that that doesn't mean that users should give up and we should not focus on other protections, because we do think this is somewhat the outlier, and there are many other protections that you can do.

So I never want to actually push a message of helplessness, but against these zero-click exploits there is very little a user can do, yes.

The Chairman. And I am not sure how much you are able to discuss in an open setting like this, but how does Google or how do other entities discover a zero-click exploit?

Mr. Huntley. So it was actually Citizen Lab that actually found this zero-click exploit and provided it to us.

The Chairman. Mr. Scott-Railton, are you able to share anything about how these things are discovered?

Mr. Scott-Railton. Yes, I am. Thanks for that question.

Citizen Lab focuses on understanding threats to high-risk groups. Sometimes these individuals come to us with a question. They feel a tickle of surveillance.

More often we go to them, and we work with them very closely to try to

understand the threats that they face. This means analyzing their devices, sometimes analyzing their network traffic.

Ultimately, it is a needle in a haystack problem.

What is interesting about this exploit is that it was found on the phone of a woman who was one of the major advocates for the women's right to drive in Saudi Arabia. And it was her vigilance and contribution to this effort of examining these cases that ultimately led to this cascade of discovery that protected over 2 billion Apple users.

Mr. Huntley. And more broadly, my team over the last 10 years have discovered over 30 different exploits being used in the wild, often against a range of platforms from a range of vendors.

And there is a range of techniques about how we find them. Often it is because the attacker makes some mistake, and so they are subject to the OPSEC restrictions as well. So they make some mistake and we are able to discover it.

In other cases, as outlined by Citizen Lab, the user is able to do some detection, and they contact us or others, and then we are able to investigate from there.

The Chairman. What would that detection look like? I mean, what would you be observing? Would you be observing your phone turning on by itself? I mean, it doesn't show any visible signs, for example, that it is recording, I assume.

[10:36 a.m.]

Mr. Scott-Railton. One of the truisms about surveillance is that people, when things happen on their phones that they don't understand, often conclude, if they are already targets of a government, that that is surveillance, which speaks to the pernicious nature of the problem.

Typically, with this pretty sophisticated stuff, there would be no sign.

There are exceptions. For example, we investigated a case where an individual was co-infected with two pieces of mercenary spyware -- Pegasus, which is made by NSO Group, and Predator, which is made by a company called Cytrox.

So it was Pegasus versus Predator on this guy's phone, and it was running hot. But beside that, usually very little evidence that a user can see.

The Chairman. And, Ms. Kanimba, who do you think is responsible within the Rwandan Government, or within Rwanda, for the use of this technology against you?

Ms. Kanimba. So within the Rwandan Government, I am not exactly sure, but I do know that they are responsible. They are the same people who kidnapped my father, who tortured my father, and who surveilled him for years, attempted to assassinate him for years.

So I have no doubt that the only government responsible for this is the Rwandan Government.

The Chairman. And with respect to everyone in government, what has the U.S. Government's response been to both your father's situation, but also the surveillance of your own phones, given, as you say, we provide a lot of economic support to Rwanda?

Ms. Kanimba. Yes. So the United States Government has designated my father as a case of wrongful detention, and Ambassador Carstens, the U.S. Special Presidential Envoy for Hostage Affairs, is dealing with my father's case.

So we are very grateful for the efforts being led by the State Department and by the SPEHA office in working to secure my father's release.

And as it relates to the spyware, I have been contacted by the FBI and other members of Intelligence, as well as in Europe, working to help protect me and help to try to make us feel safe.

However, this technology is hard to detect, and they can always reinfect my phone if they wanted to, and so I still do not feel safe.

The Chairman. And has there been any public or other response by NSO Group? They have been making the claim that their technology is not used to spy on Americans. You are an American. They spied on you, or their technology did.

Have they made any comment about the use of their technology or why they provided to it the Rwandan Government?

Ms. Kanimba. I do not know.

The Chairman. Thank you. Thank you very much.

Mr. Turner.

Mr. Turner. Ms. Kanimba, thank you so much for your compelling story and really for the heroism of your entire family.

You talked about when you were having conversations with the U.S. Government on the issues of your father and logistics and your angst that those conversations and communications would become compromised.

And I would like you to speak to that for a moment, because it really shows the expansive net that this type of spyware casts in that by infecting those who are interfacing even with our government itself, as you were relating, it makes it even a greater threat to you and your family as anyone even tries to help you.

Speak for a moment about how those communications, even the issues where you

have the private aspect of your life, you have the aspect of your family's safety, but even as you work to try to make your family more safe, you were still vulnerable.

Ms. Kanimba. Yes. Thank you for this question.

So it has been 699 days specifically that my father was kidnapped, and from the first day that we learned that he was in Rwanda my entire family stopped what we were doing and have been working very hard to try to get my father back home, calling government officials all over the United States, sending emails and talking to as many people as we possibly can.

And we know that the Rwandan Government has also been trying to stop these efforts, whether it is trying to intimidate individuals, like Congressmen and Congresswomen who are speaking out on behalf of my father on a social platform, or whether it is printing lies in the media, or whether it is just trying to really intimidate us into silence so that we do not reach all the individuals that we would like to reach to help us put pressure on the government, to let the Rwandan Government and to let my father go.

And knowing that they have been listening to these conversations, to our efforts to secure my father's release, it is our right to contact our government officials. It is our right to advocate for the human rights of my father.

And the fact that they felt they had the permission to just listen in to all these conversations and also attempt to stop these efforts from moving forward is unconscionable, and it is very scary to know that they had just this much access to us.

My father is sick now. He had a stroke recently in prison, and he now has a hanging lip. And so the urgency is here, the urgency for my father to be allowed to come home is here.

And so we know that we have to continue, we have to continue to speak out, we

have to continue our work regardless of with or without Pegasus in my phone. But this has definitely scared us and put us -- set us back in these efforts.

And in my personal, on a personal level, just the fact I am a 29-year-old woman and I use my phone quite often, not only in the efforts to secure my father's release but on my social, my private conversations with my friends, and the fact that the same government that tortured my father, that is holding him hostage, and that has been trying to silence him all these years now also has access to my private messages and my conversations and my location, it is very, very scary.

Mr. Turner. And of course that is a part of the intimidation and the attempt to control and the type of information that you would expect would be private. So thank you for your story.

John, on Citizen Lab, you were identified as being able to find some of this spyware. You cited the Commerce designation for the Entity List, and you gave some incidences of where you believe that it was working.

Do you believe it works if the Commerce Department places companies like this on the Entity List?

Mr. Scott-Railton. I was very glad to see that because I see it as a signal.

Ultimately, the Entity List is not an individual sanction. This is not a comprehensive package. Nobody is losing their rooftop swimming pool.

But it shows investors, some of whom are based in the United States -- pension funds, permanent funds -- that this industry is risky for them. And that kind of signaling, to me, is extremely powerful.

And we saw it have effect. We saw reports that the debt valuation of NSO precipitously dropped. The company now appears to be in a tailspin.

Mr. Turner. Excellent.

Shane, you made a comment that I thought was surprising. First you indicated that a lot of the times these are identified by individuals, not by Google itself.

You called on the government, the IC, to do more in identifying and countering these. But by scale, I mean, surely Google in its resources, in its interfaces, and in the work that you are doing in threat analysis, you are going to have much more information than the government does or then individuals in stumbling over these.

And I don't mean to characterize it you were saying that it is only individuals and you are not doing work, because you are.

So my question actually relates to, as you use Google's resources, as you find out this information from individuals, what is your interface with the U.S. Government?

How do you share, when you do find, and what is the work that you do with Google resources to find them, to let the IC know, the government know, the Commerce Department know, so that they can take actions beyond just the technical patches that you would be working on?

Mr. Huntley. Thanks for the question.

So I should clarify that many of these are found by -- many of these exploits are found. Like of the 30 we said, these were 30 different exploits found by us.

This specific one was found by Citizen Lab. And in some cases the users do help or point us in the direction, but we do find many of these things ourselves.

I think what you would say is that we have -- yes, I have built a great team, and Google has put a great investment in understanding these threats, and that is why we do it. And we have sort of unique visibility and we have a lot of resources that we can put against this problem.

But I always see that this, whether it is these threats or many other cyber threats, that I think taking them on has to be a team sport. And if you actually look at the

different organizations that are taking on these threats, we all have our own visibility.

So we have a lot of advantages by being Google and the platform owners and being able to do the investigation with all the technical experts we have. We do not have some of the capabilities the Intelligence Community does, and they have their unique visibility and their unique actions and things that they are authorized to do to learn information.

And similarly that organizations such as Citizen Lab and other civil society groups, they are working directly with users that are targeted. And then there are all our other industry partners and security vendors.

So there is actually very good cooperation amongst this community at present, and there needs to be that cooperation, because each of us see some part of the picture, and only by putting those pieces together and working together do we actually -- are we able to take on the adversaries and put it together.

We can't let the adversaries sort of take advantage of sort of disconnection of us only seeing part of the problem.

So when we discover things with regards to the exploits and with regards to spyware, we try to be as open as possible about publishing details so that other researchers and other entities are able to investigate further. And so we believe that shining a light on this is important.

We also work out who are the best people to contact in certain cases. So if an exploit is against Chrome or Microsoft or Apple, then we will contact them directly in the first instance to ensure that they can fix the vulnerability as quickly as possible.

But where in other cases we do make referrals through law enforcement, to the U.S. Government, where it can be disseminated further.

And we also have threat discussions with the U.S. Government and other

governments in order to take on these common threats.

And I would say the cooperation and the passing of information has gotten dramatically better over the last couple of years.

Mr. Turner. John, congratulations to you and Citizen Lab for the level of work that you are doing and the work that you are doing to make people aware of what you are discovering and what you are seeing. Great technical expertise.

You did mention the word "proliferation" at one point. So once we discover and you have discovered that this is happening -- we understand bad actors and nation-states, now we have criminal organizations, we have nonstate actors -- how do you see the proliferation of this becoming a threat and what do we do?

Mr. Scott-Railton. I see the threat from proliferation as inevitable.

When we first started working on this, we saw a handful of companies working with a handful of states. Now it is totally out of control.

It is absolutely inevitable that as more states and subnational entities gain access to this kind of technology, it will be pointed against the United States, as indeed it already has been, against the U.S. Government, and against our allies.

I also believe that it is inevitable that transnational criminal organizations and other nonstate actors will gain access to this technology. Some of it might eventually show up in ransomware with consequences for you and me and everyone else in the room.

Ultimately, I see this as a stool. There are three legs.

Civil society has been raising the alarm for years.

Tech companies for years have been trying technical control measures. Then they realized that was not enough. So they started looking to U.S. courts, beginning in 2019, when WhatsApp sued NSO. Others joined that lawsuit, and Apple followed suit

last year.

But that is not enough. We need the third leg, which is government. There is a powerful host of tools, both legislative and in terms of empowering the Intelligence Community, to disrupt and degrade the capabilities of problem actors.

Mr. Turner. Thank you. I yield back.

The Chairman. Mr. Himes.

Mr. Himes. Thank you, Mr. Chairman.

And thank you to all our witnesses, and, Ms. Kanimba, in particular, for your startling testimony.

We are doing this because we are trying to figure out what our response may be. And you gave me an idea. I don't know the ins and outs or the nuances of our relationship with Rwanda, but it seems to me that the principle that if you attack our people with these surveillance tools for nefarious ends, or any ends whatsoever, maybe not just our people but civilians or anyone else, you will not get one red cent from the American taxpayer.

You happened to have catalyzed that thought in the institution that holds the purse strings, so I thank you for that.

And I will note, your story, and stories like yours, turn our stomachs because we are a society that puts a huge premium on the dignity and the rights of the individual.

And, of course, societies that do that also tend to express their political will through democracies. And it has not come out enough today, but this feels to me like a very serious threat to our democracy and to democracies around the world which are today hanging in the balance in places like Hungary, Poland, Brazil, Philippines, and the United States if you have been watching TV over these couple of months.

You can imagine that if this can be in a warehouse in Ghana, that nobody, not

Mike Pence, not Nancy Pelosi, not Kevin McCarthy, not Adam Schiff, not the ranking member, are immune from having their most private deliberations watched.

And that may be just enough to interfere in our elections just enough to end our democracies.

John, it appalls me that there are institutions that live only because of the contract law and the rule of law in a democracy. You said that there were pension funds -- and you note in your written testimony that you think that NSO might attract venture capital from Western institutions -- you said there were pension funds that had invested in these entities. Will you name them, please?

Mr. Scott-Railton. With pleasure. Mr. Himes, thank you for that question.

The largest owner of the majority owner of NSO Group is Oregon PERS, that is the Oregon Public Employee Retirement System. Another one, Alaska's Permanent Fund.

I think that some investors have gotten into this without fully understanding what is going on, without doing the due diligence.

Mr. Himes. We will come to that.

Is that the complete list of investors that you were making reference to?

Mr. Scott-Railton. That is the complete list for NSO Group. I believe that there may be others --

Mr. Himes. What about Candiru and the other ones?

Mr. Scott-Railton. For many of those -- and this speaks to the problem of the industry -- we have no idea who some of those owners are and what that ownership looks like. But what we do know is that there have been deal after deal attempts to acquire companies like NSO backed by U.S. venture capital.

Mr. Himes. Right. Okay. So venture capitalists, name the venture capitalists that you know of that have invested in these entities.

Mr. Scott-Railton. Thank you for that question.

I think one of the biggest concerns about this technology is that sometimes the companies that are building it are just down the road from some of the capital.

For example, the owner of NSO Group, before it went to its current owner, was Francisco Partners, based in San Francisco.

Thanks.

Mr. Himes. What other ones?

Mr. Scott-Railton. That is the one that I am in a position to name right now, but happy to provide you with more.

Mr. Himes. Okay. I am going to ask you to follow up with as complete a list as possible of Western investors.

Again, the notion that you would live in the legal superstructure, with contract law and rule of law, and then use that structure to invest in a company that might end that rule of law, we need that list, because people need to get famous on this issue.

Mr. Scott-Railton. It is head scratching.

Mr. Himes. So we are talking a lot about sanctions, et cetera, but it is a truth of technology that once it is out of the bottle it is out of the bottle. If a dusty warehouse in Ghana can host one of these things, we are not putting this genie back in the bottle.

So in my remaining minute or two -- and I will open it up to any of the witnesses here -- what do we need to be doing in terms of research and development to make sure that we are technologically one step ahead of this technology?

Mr. Huntley. I can take that one briefly.

So while we can't put the genie back in the bottle, the good news on some of these exploits is that once we fix the bug being used by a specific exploit, they have to find another one.

So this a game. This is something we actually -- a race where we actually need to stay ahead.

But the investment we really need to do, and we are doing in Google and elsewhere, but we need to across the board really work on developing secure systems and making exploits harder to find. That is why we created Project Zero.

But we need investment across the board that we are building platforms where it will never be impossible but it is much harder for these vendors to find exploits, and it is much easier to detect them, and we are able to build the secure system going into the future.

Because they are investing in the research to find the holes, we need to research much more to build the more secure system so it is harder to find those holes.

Mr. Himes. I think this is really important. I will just make the observation to the many, many venture capitalist investors that are out there: We are not putting this back in the bottle any more than we are doing away with nuclear technology or anything else.

So I would suggest to these investors and venture capitalists out of here that actually developing the technology that allows this stuff to be irrelevant would be a pretty good use of their money.

Thank you, and I yield back.

The Chairman. Thank you.

Mr. Crawford.

Mr. Crawford. Thank you, Mr. Chairman.

Mr. Huntley, I am wondering if you could tell me how Google is alerted to zero-day vulnerabilities.

Mr. Huntley. Thank you, Congressman.

We have a range of different ways we are able to detect these. So one of our major projects is Safe Browsing, where we actually try and discover all forms of malicious activity on the web to protect users.

You may have seen this when trying to visit a site, and it puts this sort of big red warning, saying this site may harm your computer.

We put a lot of investment into sort of understanding what is on the internet. That is one of our primary purposes and how we build a search engine.

And one of the things we can do is to look across the entire internet looking for the malicious activity. And occasionally in this very big haystack we find the needles of these zero-day exploits. That is one way we find it.

We also have reports and details coming from our protections in Android, Android Play Protect, and we are able to get information and get reports sometimes by users about malicious activity that we find. And then our expert researchers are able to determine this is a zero-day exploit.

Mr. Crawford. How many of these come from your own hunt capability versus tips that are provided to you?

Mr. Huntley. It is hard to draw a hard line because this is very much sort of a team sport. But I would say there are 30 over the last 10 years that we have been credited for directly, and we only take credit if we were the ones to actually discover them.

Mr. Crawford. Do you receive tips from, say, for example, other tech companies, NGOs, or government entities?

Mr. Huntley. Certainly. And we said in this case we were the ones just assisting on the zero-click exploit. We definitely provide information back and forth. So we have provided information to Apple, they have provided information for us, for instance.

This is an area where we are collaborating very closely because we have a common enemy here. This isn't a matter of competition.

Mr. Crawford. Did you want to weigh in?

Mr. Scott-Railton. If the U.S. Intelligence Community, with its considerable capabilities, identified the zero-days that were being used by problem actors -- and it could -- and submitted them to big tech, you could burn their house down.

Mr. Crawford. Okay. So that brings up the next question. How would you grade the information-sharing within the industry, and between industry and the government, regarding known cyber vulnerabilities, including zero-day exploits?

Mr. Huntley. I would say the channels are there to pass the information and the collaboration. I think the biggest place this committee might want to look is actually about the release of information and how we make those balances right.

So we have this complicated, complex process that the U.S. is an offensive cyber actor in their own right and has to make complex decisions about when to keep capabilities and when to report them to get them fixed.

And I would just encourage that we do that very thoughtfully and we do that in a way which really takes into account the real risks of having exploits out there.

So I think one of the things we can push is to make sure that there is pressure on the Intelligence Community and others to report to us.

Mr. Crawford. Do you have any recommendations on how you could make the process better?

Mr. Huntley. Not specifically, since the process is relatively nontransparent to us at present. So it is hard to even determine how exactly those decisions are currently being made.

Mr. Crawford. So then making the process more transparent would be step one?

Mr. Huntley. I believe so. And also making sure that the full representation is there as well, that it is not just the people that are there doing the offensive hacking making the decision but also the people who have a full understanding of the costs potentially.

And one thing I would say is that there can be real costs. A somewhat related effort that we talked on last year is we actually discovered the North Korean Government were actually targeting exploit researchers, both from these commercial surveillance vendors but also to providers that work for Western governments.

So we know that the people that are targeting and creating these exploits are also being targeted themselves, and that is a proliferation risk in its own right.

Mr. Crawford. Got you.

Let me just shift gears real quick.

Ms. Kanimba, let me just ask you -- and this is not tech related, I am just curious -- your father, I know, is a Belgian citizen but a permanent legal resident in the United States. Had he made application for citizenship in the United States?

Ms. Kanimba. I believe he had started the applications, yes.

Mr. Crawford. And just curious, when did he start that application process?

Ms. Kanimba. It was in 2020, beginning of 2020.

Mr. Crawford. So basically the same year he was abducted then?

Ms. Kanimba. That is correct.

Mr. Crawford. Do you think that was a contributing factor to their decision to abduct him, prior to him becoming a U.S. citizen?

Ms. Kanimba. That is a possibility. But we know that for many years they had targeted him and attempted to assassinate him. And kidnapping just was an added -- and the incarceration was the last drop.

Mr. Crawford. Well, thank you for being here. I appreciate it.

Yield back.

The Chairman. Mr. Carson.

Mr. Carson. Thank you, Chairman.

Ms. Kanimba, we are thankful for your efforts to not only free your dad but to raise awareness of the monitoring of the Kagame government.

In America we at least try to walk the line, the fine line between providing for the security and safety of our citizens but not impeding on anyone's First Amendment rights.

What is your perspective, ma'am, on the monitoring of domestic terrorists intent on harming us versus those like yourself who are fighting for human rights?

Ms. Kanimba. I am sorry. Can you repeat the question?

Mr. Carson. What is your perspective on monitoring and tracking domestic terrorists intent on causing harm to people in a traditional context versus those like yourself who are fighting for basic human rights?

Ms. Kanimba. So my story has just -- my experience has been about, of course, standing up for the human rights of my father. I am not an expert in policy. I am an expert in what has happened to my father, in following it.

What I know is that Americans need to feel safe. We need to feel safe in our country. We need to feel safe when we travel. And the spywares, like the NSO's Pegasus spyware, are not something that help -- is not something that has helped me feel safe.

At least knowing that the Rwandan Government and the repressive regime is able to get their hands on this software and use it against us is scary.

However, in terms of how to monitor security in the United States, I wouldn't be able to advise on this.

Mr. Carson. Well, thank you.

Mr. Railton, what is your perspective, sir, on other nations using Pegasus to monitor U.S. citizens at home and abroad?

Mr. Scott-Railton. Thank you for your question, Mr. Carson.

When confronted with abuses the mercenary spyware industry typically has a message: Our technology is designed to fight crime and terror. Period.

But the facts don't bear this out, in two ways.

First, abuses have been a feature of this technology and industry since day one.

Second, and as we have discussed today, the crime and terror narrative omits the fact that a significant proportion of the use that we see of mercenary spyware is state-on-state espionage, governments targeting other governments. And of course the United States has been one of those targets.

Mr. Carson. Thank you, Chairman. I yield back.

The Chairman. Mr. Mullin.

Mr. Mullin. Thank you, Mr. Chairman.

Mr. Huntley, you might have answered this question already, but maybe I was just over here doodling on a piece of paper and I didn't understand it. But what size is Google's Threat Analysis Group, TAG?

Mr. Huntley. So we are one small part, just over 50 people, but we are like a very small part that actually is supported by many thousands of people across the company that are working on security and security issues.

We are there to sort of like identify and provide some deep expertise on these threats. But we also, as I mentioned, work very closely with Project Zero, Chrome security, Android security, the people securing our own systems, Safe Browsing.

So the overall effort on security that actually in some ways contribute to this is

very huge.

Mr. Mullin. So it is a team effort, but the serious issues come to you, to the group of 50?

Mr. Huntley. My team is specifically focused on gaining that understanding of adversaries. We are the people who are built to be the experts on the threat actors and able to provide that information about what they are doing.

And one of the biggest outcomes of that is so we can actually use that to defend our products, make our products more secure, and actually make changes across the ecosystem.

Mr. Mullin. So when did TAG get stood up?

Mr. Huntley. So my team was formed in 2010, 12 years ago, and I was there at the founding. It actually sprung out of Google being targeted by China in an incident called the Aurora incident in 2009.

And at that time, Google was quite forward-leaning in deciding that it really needed a rather professional team working on this, fully dedicated, and then the team was founded then.

Mr. Mullin. Do you know the amount of resources that Google puts towards this?

Mr. Huntley. It is I think -- I can take that on notice, but it is very difficult to add up because there is no, like, hard boundaries about where these things start and end. But I do believe it is like -- it is not cheap. We compensate our people well, we put a lot of resources, we put a lot of computing resources.

Mr. Mullin. But my point on that is, Google is taking this very serious?

Mr. Huntley. Yes.

Mr. Mullin. And you guys are devoting your own personal capital to go after

this?

Mr. Huntley. Absolutely. And we see that keeping users safe is a key part of not just the moral implications, which are very clear by the testimony today, but also the commercial implications of the tech industry and our society and the economy in general has to rely on a secure system.

Mr. Mullin. Does Google have a policy in place to alert customers or others? And how do you go about that?

Mr. Huntley. Yeah. Actually we just hit the 10-year anniversary of a program that I developed, that we set a policy 10 years ago that whenever we detect a user that is being targeted by a government-backed threat, whether it was successful or not, we provide a prominent warning that they are the target of government-backed threats, and we actually provide them specific security advice.

We want to make sure that we never are in the position where we know that a user is being targeted by a government threat and that user doesn't. So we believe we have a moral imperative to tell those users.

Mr. Mullin. Mr. Scott-Railton, I was coming to you next.

Mr. Scott-Railton. Thank you, Mr. Mullin.

I have an observation about those notifications. They are great for us as researchers because when they land on people's phones they know something has happened, they need to take some action.

But I believe that the industry still must do more. One challenge with those notifications is that users are typically not provided with any information about who did it, how, or when.

I understand the industry faces many challenges around disclosing some of their sensitive methods for identifying threat actors, but unfortunately I think there is more

that can happen with the notification so that victims know who to look to for who is responsible and to hold people accountable for it.

Mr. Mullin. So earlier in your testimony you had said that you identified targets, vulnerable individuals, and then you alert them.

How do you do that? How do you know which ones are the most vulnerable? And then how do you --

Mr. Huntley. Are you speaking to me, Congressman, or not?

Mr. Mullin. No, I am talking to Mr. Scott-Railton.

Mr. Scott-Railton. One of the ways that we identify potential targets is the same way that the governments that target them do: Who is in the press criticizing them? And sure enough, if you talk to those people, there is a good chance they get targeted. There is a good chance that high-profile dissidents and human rights defenders, especially in repressive regimes, get targeted.

But sometimes we are in a position to work with large sets of targeting information. That happened in 2019 when WhatsApp asked us to help understand an attack against their users. And that is how we saw a full set of targeting, including a lot of government-on-government targeting.

Mr. Mullin. Mr. Huntley.

Mr. Huntley. From our perspective, we have the advantage and visibility of our scale. We are able to see some of the times the large-scale operations of these actors against our users.

And then we are able to put the pieces together, and we are able to sort of expand out and understand the scope of what these actors are doing. And then we have a team dedicated to this, and every single user gets the warning.

Mr. Mullin. Thank you, Mr. Chairman. I yield back.

The Chairman. Thank you.

And just so members know, we are in the middle of the first vote, and we will go up until we think we need to recess and then we will come back.

Representative Speier.

Ms. Speier. Thank you, Mr. Chairman.

Thank you all for your testimony.

Ms. Kanimba, your testimony was riveting, and we need to take action to get your father out of prison. And I would concur with Mr. Himes. I think recalling the funds, foreign aid, would be a good step in that direction.

You are a U.S. citizen, correct?

Ms. Kanimba. That is correct.

Ms. Speier. And yet you were, in fact, spied on, and NSO says that they do not spy on U.S. citizens.

Mr. Scott-Railton, in the course of your research, have you identified additional American citizens or U.S. Government officials infected by Pegasus or another company's spyware?

Mr. Scott-Railton. In the course of our research we have identified the targeting of other U.S. citizens.

Ms. Speier. Can you name them, please?

Mr. Scott-Railton. The citizens who were targeted?

Ms. Speier. Yes.

Mr. Scott-Railton. In some cases I am not able to do that because we have a responsibility of confidentiality. But I would be more than happy to provide a list of public reporting of the many U.S. citizens who have been targeted over the years.

It goes back to Americans working in nonprofits in Mexico, supporting local

groups, to people working on electoral consulting in places like Panama, right up until the present.

Ms. Speier. How about public officials?

Mr. Scott-Railton. I am not in a position to talk about other American public officials. But I will highlight, with a big underline under one category, which is American journalists regularly get targeted with Pegasus.

Ben Hubbard would be a good example. He was targeted not once but two separate times, and in fact the second time he was targeted it was after the fact of his targeting had been publicly reported.

Ms. Speier. And Jamal Khashoggi was targeted as well, was he not?

Mr. Scott-Railton. Both Jamal's wife and his fiancee were targeted with Pegasus spyware. This is not uncommon to see targeting around a person. In the case of Jamal specifically, we don't have access to a device in order to do that analysis.

Ms. Speier. All right.

Should the DNI or Commerce make the list public of these companies?

Mr. Huntley. I see no reason why not to make this public. I think drawing attention where we can to who we consider these threats are, I think, as Mr. Scott-Railton spoke about, it is like that sends a lot of message.

And I think it is about incentives as well, and I think one of the incentives that I have been pushing when I have been speaking externally is also on the talent as well.

I want to make it so that people think twice before accepting jobs with them or with putting their careers or their reputation on working with these companies.

If you are a talented security researcher, I want to make it so you really think twice before accepting a job with someone like NSO and you do something more productive with your life.

Ms. Speier. Mr. Huntley, do you believe the NSO's public claims that it does not have access to any of the data that its customers gather with Pegasus?

Mr. Huntley. I would be struggling to find direct evidence, but tangentially I find that difficult to believe.

This also seems, from my perspective, or from the outside, it seems that there are sort of conflicting claims as well. They both seem to be making strong claims about how they are controlling the use of their technology but also having no visibility of how the technology is used.

And I can't understand how you can make both claims at the same time. They are either handing full control over to their end users in which they are making -- then the decision is on them, and they do not have any visibility, or they are actually enforcing strong controls. I don't see how they can be doing both.

Ms. Speier. What can companies like Google do to protect users from these threats?

Mr. Huntley. I think, as I spoke, the biggest things we can do at the moment, at least some of those things, is we build secure platforms. We are working tirelessly to make Android, Chrome, all our other products more secure so it is harder for these companies to target them.

We brought protections into the Android operating system, Google Play Protect. We are making it more difficult for them to operate.

And then a very small part of the work, as the team, my team does, of trying to understand everything possible we can do about the specific threats and then taking them on individually to sort of deny them the use of vulnerabilities, malware, and to actually build specific protections against their actual technology.

Ms. Speier. Can you build a way that the average consumer can go to a website

and determine whether their phone is being spied on?

Mr. Huntley. I think it is a very difficult ask, and I think it is very hard to do in a comprehensive way, because as soon as you make it super public way like that, then we know that the NSO people will be testing against as well.

So we always -- we are not claiming we actually have perfect understanding as well. So at the moment, some of these -- we can produce some scanning. We deploy some of it to scale too.

If we are able to detect it on every phone, and in some cases we can, we don't wait to create a website or make it so the user has to do something. We push these protections into the protections on the phone, such as Android Play Protect.

Ms. Speier. Yes, Mr. Scott-Railton.

Mr. Scott-Railton. Pegasus, like other viruses, has a different feature than going after, for example, trying to find a bacteria or an infectious disease, which is it can read the papers. And when companies produce tools to detect Pegasus, the first thing that happens is those companies engineer their products to avoid them.

This is part of why it is so hard for the anti-virus industry model, for example, to find this stuff and why it really requires serious government action.

Ms. Speier. Thank you. My time has expired.

The Chairman. Mr. Gallagher.

Mr. Gallagher. Thank you all for being here and discussing this important topic.

When we talk about commercial spyware, I think we need to broaden the aperture to also include software like WeChat, TikTok, and other Chinese apps where we have increasingly compelling evidence that the Chinese Communist Party is collecting or censoring information.

It is also worth bearing mention that through its Digital Silk Road, in particular, the

CCP is exporting surveillance technologies through proxies Huawei, ZTE, Hikvision, just to name a few.

And the goal is to create client authoritarian leaders who owe much of their ability to monitor and oppress their populations to the Chinese Communist Party and its technologies.

I know that Citizen Lab has done a lot of great work on WeChat in particular. There was a recent report on WeChat where you found that, quote, "WeChat communications that are conducted entirely among non-China registered accounts are subject to content surveillance, and, in fact, can contribute to further oppression in China."

I understand this was not yours but one of your colleague's reports, but I was hoping you could speak a bit more about the threat as you see it posed by software such as WeChat's.

Mr. Scott-Railton. Well, thank you for that question. It is, indeed, my colleague's work.

I would say the take-home discovery there is that we found that users of non-Chinese versions of WeChat, their communications with each other were mined to train the censorship system used against Chinese users.

So people in democracies having their communications mined for censorship back home and the increase of authoritarian activity there.

Mr. Gallagher. Thank you.

Additionally, the report -- again, I recognize it is not one that you authored, but you are well acquainted with it -- concluded that future work is required to understand if this behavior is unique to Tencent or if it is common for internationally operating Chinese social media companies to use communications among their non-Chinese users to

implement Chinese political censorship, which is related to the point you just made.

So I assume you agree that is an area that bears further examination, talking more about the role that Chinese software, particularly apps like TikTok, could play in contributing to CCP surveillance or influence globally.

Mr. Scott-Railton. As you said, Mr. Gallagher, not really my area, but in general I agree this topic deserves much scrutiny.

Mr. Gallagher. Could you talk a bit about -- actually maybe a question for Mr. Huntley -- talk a bit about how the Threat Analysis Group approaches Chinese software apps like TikTok or WeChat?

For example, do you conduct any sort of vulnerability analysis surrounding these type of apps? Does your feedback play a role in terms of which apps might be available for download, for example, in the Android store?

Mr. Huntley. Thanks for the question, Congressman.

So we certainly have -- one of our goals is to actually look at security across the board, both for our users, which we have our corporate users of over 100,000, and also for the internet at large.

We have multiple programs to actually look for vulnerabilities in software. And Project Zero is actually I think a leading effort where they actually don't just look at our own products but actually look at products across the board, looking for vulnerabilities, and have published research on many, many different areas, and those would be in scope to examine as well.

And also we have -- try and maintain -- we maintain strong restrictions on sort of what software can go into the Play Store, and if vulnerabilities or things are operating outside privacy guidelines, then they are subject to removal.

Mr. Gallagher. Do you think TikTok is a threat?

Mr. Huntley. I certainly don't use it, but I am not outside the targeting demographic, but --

[Laughter.]

Mr. Gallagher. You don't need to answer that one.

Mr. Huntley. I think it is worth examining. I think it is -- I don't think it is my place to speak on a competitor in this place, but I think it is -- you raise points. It is very much worth examining under what rule of law they are operating.

Mr. Gallagher. Well, I think the evidence is mounting to suggest that it is, as well as what we know about the company that owns TikTok. I believe TikTok is the most popular social media app in the United States right now.

So in a very real sense, when we look at the Chinese Communist Party's strategy, it has been one not only of military intimidation in the South China Sea or economic coercion against Taiwan or other countries that recognize Taiwan, but a united front strategy aimed against America that is addicting millions of Americans -- whether intentional or not -- addicting Americans to cheap Chinese goods, money from China, addicting Americans to fentanyl with precursors made in China, and addicting America's kids to an incredibly addictive social media app, which is not good for them, destroying their brains.

I hate to sound like the old buzzkill in the room. I used to be like the youngest Member of Congress.

The Chairman. The young buzzkill.

Mr. Gallagher. Exactly. It should be the young buzzkill. That is right. That will go on my gravestone.

But my time is expired. Thank you, Mr. Chairman.

The Chairman. Hate to cut you off on that note.

Mr. Castro and I think -- well, we will see how many are yet to vote. We still have about 320, and hopefully we can get to Mr. Maloney as well before we recess.

Mr. Castro. Sure. Thank you, Chairman. Thank you, Chairman Schiff, for holding this important hearing, and also to our witnesses for your testimony.

Ms. Kanimba, your father, Paul Rusesabagina, is a resident of San Antonio and a constituent of mine, and for 2 years my staff and I have worked with you and your family to secure his release from prison in Rwanda.

This month, the House of Representatives passed a bipartisan resolution condemning his arrest and calling for his release on humanitarian grounds.

I raise this because NSO Group claims its spyware cannot be used against Americans, and you said earlier very clearly that you are an American citizen. Your experience is clear evidence that this is simply not true, as does the experience of U.S. diplomats in Uganda and other locations who had their phones hacked with NSO spyware.

And you mentioned in your opening statement that Belgian intelligence, among others, confirmed that your phone was compromised.

And the forensic evidence that you submitted for the record indicates that your phone was accessed numerous times on and before April 2021, that that timeline matches up with the specific email communications between my staff and you regarding what actions I and other Members of Congress were taking to raise your father's imprisonment with the Rwandan Government, the FBI, and this committee.

We have seen the reports that this software was used against U.S. State Department employees also in Uganda. It is clearly being used against human rights and civil society activists such as yourself.

Your testimony today raises a prospect that communications between Congress,

you, and your lawyers may have also been wrongfully accessed by the entity that targeted you with Pegasus.

And after news about Pegasus broke, I worked with my colleagues, including Rep. Malinowski, to urge the Commerce Department to put the NSO Group on the Entity List, which would block them from doing business with the United States.

In response to our inquiry, the Commerce Department did just that in November of 2021.

It is essential that the NSO Group remain on the Entity List given their role in enabling surveillance of U.S. citizens.

And, Ms. Kanimba, the NSO Group claims that their software was sold to countries like Rwanda for law enforcement purposes.

Given the Kagame regime's abysmal record on human rights and the rule of law, do you think the NSO Group could seriously have believed that the Rwandan Government wouldn't abuse this software or is it just a convenient excuse?

Ms. Kanimba. Thank you very much, Congressman. And thank you so much for all the work that you have done with our family to help save our father's life.

I believe that the NSO Group must not be telling the truth about Rwanda and its use of the software. Rwanda is reported as having -- many reports have been written about Rwanda's human rights abuses by the United States, by human rights organizations, and by many people across the world, including victims like ourselves.

And so it is a known fact that the Rwandan Government perpetrates these abuses internationally. And most recently the Freedom House released a report on transnational repression detailing how the Rwandan Government perpetrates transnational repression on U.S. soil.

So I believe the NSO Group must know this.

Mr. Castro. Thank you.

Mr. Scott-Railton, I know Mr. Himes asked about investors in these companies. I want to ask you about the host nations. What are the leading host nations for these spyware companies?

Mr. Scott-Railton. Mr. Castro, thank you for your question and for your continued focus on this critical issue.

It is an interesting thing that over the last decade we have seen the centers of gravity move in the spyware world. A decade ago we were looking at companies with names like Hacking Team, based in Italy, FinFisher, Germany, the U.K., and more.

Today, one area that many have heard about is Israel, which has a vibrant tech sector and has become a market leader in many interesting areas of technology, including spyware.

Another, which many are less familiar with but which plays an outsized role in providing safe havens for problematic companies, is Cypress, through which many concerning transactions and pieces of spyware pass.

In both cases and more -- Bulgaria would be another, Cytrox, Macedonia -- these are countries that could do a lot more to rein in their industry.

Mr. Castro. I was going to ask, what are the countries doing? What are any of the countries doing to combat this?

Mr. Scott-Railton. Well, let's take Cypress. I don't think they are doing very much, frankly, and it strikes me as an area where serious diplomatic efforts would be extremely helpful.

When it comes to Israel, they have an export control authority. That authority has authorized many of the sales that have led to these problematic cases. And so I think there, too, there is an opportunity for diplomatic engagement and pressure.

Mr. Castro. Thank you.

I am out of time, and I yield back, Chairman.

The Chairman. Thank you. And thank you, Mr. Castro, for all your work on this issue. Greatly appreciate it.

Mr. Sean Patrick Maloney.

Mr. Maloney. Thank you, Mr. Chairman. And I will try to be brief since we are under time pressure on the vote. And I want to add my thanks and admiration for Ms. Kanimba.

Your story is extraordinary, and we are all proud of you. And I want to ask you what actions, if any, the U.S. Government is not taking that you would like it to take.

Ms. Kanimba. So I just want my father home. I hope the U.S. Government will do everything possible to bring him home before it is too late. Thank you.

Mr. Maloney. Fair enough.

To our other witnesses, thanks for your work.

Obviously, I assume you are supportive of the provisions in the IAA that would try to get at this problem and some of the information around it.

But if you were writing the law and you could pass any provision you wanted, what would you have the U.S. Government do beyond what is in the IAA?

Mr. Scott-Railton. Well, I don't write laws and I am not a lawyer.

But what I will say is one area that seems to me to be critical is encouraging the Intelligence Community to identify and disrupt the activities of these companies. That seems like a real opportunity.

Another area that is critical, right now doing business with the Federal Government, getting acquired by a U.S. company, or even doing business with an American police department is the golden prize for many in the spyware industry.

As long as that remains as a possibility for problematic actors, they are going to get support from investors, because that is the prize. If we can chill that, if we can make it clear that the door closes, then we can accomplish a lot.

So I would encourage Congress to look at all of those issues as ways to engage.

Mr. Maloney. And wouldn't the foreign market be large enough? Even among all those entities, even if it was just non-U.S, why would that chill their business model? These aren't U.S. companies.

Mr. Scott-Railton. This is a very interesting question.

One of the interesting features of the spyware industry that we have learned from public reporting is that companies like NSO tend to soak their Gulf clients, charging them hundreds of millions, while charging European countries tens of millions, if that, according to public reporting.

Presumably, it is in the business interest of many of these companies to try to have their cake and eat it too, to get business in the United States, to get business in Europe, and to continue the money flow from problematic actors.

That U.S. business legitimizes what they are doing, and it is something that they can take to investors to say, look, the U.S. Government is not going to be on our back, we are working with them, we are selling to American police departments.

If you can cut that possibility off, I think you can have tremendous impact.

Mr. Maloney. Are you aware of any contracts of that kind?

Mr. Scott-Railton. We know that the FBI acquired --

Mr. Maloney. Beyond the FBI case, which I know. It has been well documented. What about anybody else?

Mr. Scott-Railton. We know that NSO Group has made extensive efforts to sell to U.S. police departments, but I am not aware of any other contracts at this time.

Mr. Maloney. Any evidence of these tools being used in the conflict in Ukraine?

Mr. Scott-Railton. None that I am aware of.

Mr. Huntley. No, Congressman.

Mr. Maloney. All right. Well, thank you very much.

And I yield back, Mr. Chairman.

The Chairman. Thank you.

I want to thank our distinguished panel of witnesses for appearing before the committee today. The implications of what you have shared are profoundly troubling for our national security and for free and democratic societies around the world.

Your testimony only reinforces our strong conviction that the United States and other like-minded countries must act in concert and with a greater sense of urgency to stop the spread of foreign spyware and before that window to act closes.

Numerous organizations have contacted the committee regarding the topic of foreign commercial spyware, including underscoring the relevance of our ongoing oversight.

One company, Microsoft, was unable to send a representative to testify today but submitted a written statement for the record. I ask unanimous consent for Microsoft's statement to be added to the record.

[The information follows:]

******** COMMITTEE INSERT ********

The Chairman. With that, I want to thank you once again for your testimony.

And the committee stands adjourned.

[Whereupon, at 11:28 a.m., the committee was adjourned.]