S. HRG. 118–446

CYBERSPACE UNDER THREAT IN THE ERA OF RISING AUTHORITARIANISM AND GLOBAL COMPETITION

HEARING

BEFORE THE

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC, AND INTERNATIONAL CYBERSECURITY POLICY

OF THE

COMMITTEE ON FOREIGN RELATIONS

UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 24, 2024

Printed for the use of the Committee on Foreign Relations

Available via http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
57–143 PDF WASHINGTON : 2024

COMMITTEE ON FOREIGN RELATIONS

BENJAMIN L. CARDIN, Maryland, *Chairman*

JEANNE SHAHEEN, New Hampshire	JAMES E. RISCH, Idaho
CHRISTOPHER A. COONS, Delaware	MARCO RUBIO, Florida
CHRISTOPHER MURPHY, Connecticut	MITT ROMNEY, Utah
TIM KAINE, Virginia	PETE RICKETTS, Nebraska
JEFF MERKLEY, Oregon	RAND PAUL, Kentucky
CORY A. BOOKER, New Jersey	TODD YOUNG, Indiana
BRIAN SCHATZ, Hawaii	JOHN BARRASSO, Wyoming
CHRIS VAN HOLLEN, Maryland	TED CRUZ, Texas
TAMMY DUCKWORTH, Illinois	BILL HAGERTY, Tennessee
GEORGE HELMY, New Jersey	TIM SCOTT, South Carolina

DAMIAN MURPHY, *Staff Director*
CHRISTOPHER M. SOCHA, *Republican Staff Director*
JOHN DUTTON, *Chief Clerk*

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC, AND INTERNATIONAL CYBERSECURITY POLICY

CHRIS VAN HOLLEN, Maryland, *Chairman*

JEFF MERKLEY, Oregon	MITT ROMNEY, Utah
BRIAN SCHATZ, Hawaii	TIM SCOTT, South Carolina
TAMMY DUCKWORTH, Illinois	BILL HAGERTY, Tennessee
CHRISTOPHER A. COONS, Delaware	PETE RICKETTS, Nebraska

C O N T E N T S

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

CYBERSPACE UNDER THREAT IN THE ERA OF RISING AUTHORITARIANISM AND GLOBAL COMPETITION

TUESDAY, SEPTEMBER 24, 2024

U.S. SENATE,
SUBCOMMITTEE ON EAST ASIA, THE PACIFIC,
AND INTERNATIONAL CYBERSECURITY POLICY,
COMMITTEE ON FOREIGN RELATIONS,
Washington, DC.

The committee met, pursuant to notice, at 10:04 a.m., in room SD–419, Dirksen Senate Office Building, Hon. Chris Van Hollen presiding.

Present: Senators Van Hollen [presiding], Helmy, Romney, and Ricketts.

OPENING STATEMENT OF HON. CHRIS VAN HOLLEN, U.S. SENATOR FROM MARYLAND

Senator VAN HOLLEN. This meeting of the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy will come to order.

I would like to begin by thanking Ranking Member Romney—Senator Romney—for your partnership in convening this hearing to discuss threats to cyberspace and internet freedom in an era of rising authoritarianism and global competition.

We are grateful to be joined by an experienced panel, including Laura Cunningham, the president of the Open Technology Fund; David Kaye, a clinical professor of law at UC Irvine; and Jamil Jaffer, the executive director of the National Security Initiative, all of whom I will introduce a little more fully in a moment.

At the beginning of this century there was optimism about the democratizing power of the internet. Technologies that we now take for granted such as the internet itself, social media, and smart phones were revolutionary, helping connect humankind in unprecedented ways and creating opportunities for people to challenge authoritarian and repressive governments.

We saw these technologies used by the 2009 green movement in Iran and then the Arab Spring as well as other digitally organized demonstrations around the world, and these technologies continue to hold that promise.

But the use of these technologies to enable protest movements and dissent prompted a backlash from authoritarian governments who recognize that digital connectivity in the hands of their peoples could pose a threat to their grip on power.

As a result, these regimes and repressive governments quickly sought to develop methods to restrict the free flow of information, to limit political discourse online, and to suppress freedom of expression including, in many cases, seeking to silence their expat and diaspora communities abroad. To do so these governments turned to a host of technologies to track and disrupt dissent.

Fast forward to today, and we have witnessed an explosion of new technologies and practices such as internet shutdowns, censorship techniques, mass surveillance, and facial recognition technologies, commercial spyware, and other tools that are used to suppress public dissent. And sadly, in many ways repressive regimes are succeeding in this space.

According to Freedom House's 2023 "Freedom on the Net" report, global internet freedom has declined for the thirteenth consecutive year in a row.

The commercial spyware marketplace where shady private companies sell hack for hire technologies used against human rights defenders is booming. Some estimates suggest it is a $12 billion industry.

The proliferation of AI enhanced mass surveillance technologies spread by nations like the PRC and others is accelerating as regimes seek to engage in the mass surveillance of their citizens.

This alarming trend presents significant challenges not only to individual privacy, but also to global security, to democratic governance, and freedom of expression. The tools designed to empower citizens are being weaponized against them, and we must take decisive action to counter this trend.

Furthermore, countries like the People's Republic of China are capitalizing on this trend by exporting mass surveillance technologies globally, offering tools that enable oppressive regimes to monitor and control their populations.

Meanwhile, according to a recent report from the Atlantic Council's Digital Forensic Research Lab, companies in India, Israel, Italy, and other countries have been marketing their spyware to oppressive governments.

This proliferation of surveillance capabilities in spyware not only exacerbates human rights abuses but also sets a dangerous precedent for how technology can be used to undermine democratic movements worldwide.

These threats are already being keenly felt by civil society organizations who seek greater transparency and accountability from those in power, and if left unchecked they will continue to have a chilling effect on dissent and undermine privacy and democracy movements worldwide.

While predominantly used by authoritarian governments, the last decade has seen aspects of digital authoritarianism creep into democratic states, accelerating global trends of democratic backsliding.

Democracies are not immune to the allure of these technologies, and while there are legitimate law enforcement uses for many of them, we should ensure that our democratic partners and allies respect human rights and remain true to the values that bind us together.

As authoritarian and repressive governments deploy technologies to suppress dissent, we need to find ways to counter their efforts so technologies can be used in a way that sustain and support democratic values and norms rather than undermine them.

This includes initiatives to strengthen internet freedom and combat internet censorship; better protect activists, journalists, and human rights defenders from cyber threats, harassment, and abuse; sanctioning companies that sell spyware to authoritarian regimes that use it to prey on their citizens; and shaping emergency technologies like AI powered mass surveillance technologies so they deliver services that are in line with our values.

I want to applaud the Biden administration for taking a series of actions in this space designed to stem the tide of digital authoritarianism.

On internet freedom the Administration has worked closely with the Open Technology Fund to provide tens of millions of dollars to enable tens of millions of people living in autocracies to use virtual private networks and other technologies to circumvent government censorship. And on commercial spyware the Administration has used many of the tools in the executive branch's toolkit including executive orders, sanctions, visa restrictions, export controls, and diplomatic agreements to tackle an industry that is out of control.

These efforts to protect the free flow of information are crucial to keeping pace with the rapid advancement of technologies designed to crack down on political dissent. We must continually assess the effectiveness of government action and adapt our strategies to combat these threats to democracy and human rights.

Congress should also consider how we can best direct and empower the executive branch to tackle these issues. Every year the State Foreign Operations appropriations bill funds internet freedom programs at the State Department as well as the Open Technology Fund, but we must think creatively about what other legislative tools we can deploy to counter these growing threats.

As we navigate the challenges of digital authoritarianism, we must remain vigilant, for the technologies designed to connect us can easily become instruments of oppression.

If we do not act now we risk descending into an Orwellian nightmare where surveillance and control overshadow our fundamental freedoms.

I am glad that we have an excellent panel here today to help us think through these issues and what Congress could potentially do about it.

Before I turn it over to the panel let me turn it over to Ranking Member Romney. I do want to take this opportunity to again thank him for his partnership on this subcommittee. It has been good to team up with him on a number of pieces of legislation, some which have passed already, some which have not yet.

But thank you, Senator Romney, for your leadership and your service, and with that let me turn it over to you.

STATEMENT OF HON. MITT ROMNEY,
U.S. SENATOR FROM UTAH

Senator ROMNEY. Thank you, Senator Van Hollen, and witnesses for being here today. I likewise am disturbed by the threat posed

by technology and particularly in the area of cyber intrusion warfare, oversight, spying, and so forth.

I guess it is no surprise that systems that are in conflict—free nations versus authoritarian nations—would find that the competition goes beyond air, land, and sea and is now also in cyber.

You have to count me, however, as skeptical that there is something we can do to prevent the bad guys from doing bad things. It strikes me that they will use every tool available, and now there is a whole host of new tools associated with cyber and AI and quantum and so forth that they see as vehicles to do what they want to do.

I do not know if there is any way we can prevent them from doing that, other than by developing tools ourselves that are superior to theirs and staying ahead.

Telling them, no, you cannot spy on your people is simply going to be laughed at because they will spy on their people. Telling them, no, they cannot spy on us, no, they will laugh at that.

They will even use balloons to spy on us. But that is, of course, an outmoded technology, but the modern technologies they will use and abuse to the extent humanly possible, and I do not think there is anything we can do that will keep the authoritarians from doing awful things.

Look at Russia. They just invaded a sovereign nation and are killing and maiming hundreds of thousands of people. So sanctions by American businesses or by the American government or our calling for freedom of the airwaves and prevention of censorship strikes me as making us feel good that we are saying things, but they are going to keep doing things that are detrimental to the freedom and human rights that exist in our nation and in other free nations.

So I am very interested in hearing what you all have to say about what actions we can take to do a better job securing our freedoms and preventing the authoritarians from taking advantage of the technologies that are suddenly available to them.

I would note that particularly with the advent of AI and the leaps and bounds that it is predicted to take over the next 4 to 5 years, creating super intelligence, as we heard Sam Altman say just yesterday, within the next thousand days, with the advent of that technology and potentially quantum computing, what do free nations do to secure the rights that we hold so dear?

And again, it strikes me that the way that we secure those rights is by being superior and having technology which is able to combat theirs with its superiority, and doing what America has always done, which is out innovate and out invest our adversaries, and by holding aloft the flame of freedom.

With that, Mr. Chairman, we will turn to the panel and hear what their thoughts might be.

Senator VAN HOLLEN. Thank you. Thank you, Senator Romney.

I am going to introduce each of you, and then we will have you go in turn.

Ms. Laura Cunningham is the president of the Open Technology Fund which is a congressionally authorized and funded nonprofit that seeks to advance internet freedom in repressive environments.

She has a decade of experience working on internet freedom, and prior to her time at OTF she was at the State Department's Bureau of Democracy, Human Rights, and Labor where she led the department's internet freedom programs.

Welcome.

We also have with us Mr. David Kaye who is a professor of law at the University of California Irvine. From 2014 to 2020 he served as the United Nations special rapporteur on the promotion and protection of the right to freedom of opinion and expression.

In this role he focused particularly on issues related to freedom of expression and technology, and his book entitled "Speech Police: The Global Struggle to Govern the Internet" explores the ways in which companies, governments, and activists struggle to define the rules for online expression.

We are also very pleased to be joined by Mr. Jamil Jaffer, who is an alumni of this committee. He is now the founder and the executive director of the National Security Institute at the Antonin Scalia Law School at George Mason University, where he also serves as an assistant professor of law.

He is also a venture partner with Paladin Capital Group, and prior to his current work he was a staff member, as I said, here on the Senate Foreign Relations Committee and on the House Permanent Select Committee on Intelligence.

I thank all of you for being here. I respectfully ask that you try to keep your opening statements to the 5 minutes, and if you cannot cover something there, we will certainly get to it in the questions.

With that, let me turn it over to you, Ms. Cunningham.

STATEMENT OF LAURA CUNNINGHAM, PRESIDENT, OPEN TECHNOLOGY FUND, WASHINGTON, DC

Ms. CUNNINGHAM. Chairman Van Hollen, Ranking Member Romney, thank you for inviting me to testify today on the threat of digital authoritarianism.

Today two-thirds of the world's population—nearly 5 ½ billion people—live in a country where the global internet is censored, and this number is only increasing as authoritarians harness technological advances to increase the scale, scope, and efficiency of digital repression.

But this is not merely a technical challenge. It is a normative contest to determine whether governments use technology to entrench authoritarian control or empower democratic freedoms.

The Open Technology Fund was established over a decade ago with bipartisan support from Congress to combat digital authoritarianism. To do this we support open source tools that provide secure and uncensored access to the internet.

Today, over 2 billion people globally use OTF funded technology. OTF's primary focus is on the human rights abuses that result from the application of repressive technologies.

However, the threat I want to focus on today is the digital authoritarian model that information control technologies have enabled and not merely the technologies themselves.

Worldwide, more governments are substituting repressive technical shortcuts for the hard work of good governance to control their populations in ways that were previously unimaginable.

This is the greatest danger to democracy of our time with profound implications for our democratic principles, national security, and global economic competitiveness.

Online censorship has become the cornerstone of digital authoritarianism, facilitating easy and effective information control to eliminate government accountability and obfuscate the truth.

We all know this is the case in China and Iran, but it is being normalized in dozens of countries around the world. And autocrats are forging ahead with even more blunt censorship techniques including total internet shutdowns.

In fact, last year 39 governments shut down the internet over 280 times. To further enhance their control authoritarians are also leveraging AI to increase censorship's scale, speed, and efficiency.

Leading digital authoritarians have also normalized the use of sophisticated surveillance tools to intimidate, imprison, and stifle domestic political opposition. In fact, research supported by OTF found that over the last decade more than 110 countries received information control technologies from China or Russia.

In addition, Huawei has built over 70 percent of Africa's 4G networks, and with such powerful tools few authoritarians are willing to stop at their own borders.

Commercial spyware products, which have been acquired by nearly 40 percent of all nations, have now made it possible to surveil citizens anywhere in the world. This could convince some that technology is inherently oppressive, but nothing could be further from the truth.

The internet offers extraordinary potential for global connection, inclusive democratic participation, and economic growth at a speed and scale unprecedented in human history.

The reality is that a free and open internet meaningfully improves the lives of billions of citizens around the world. It is clear that the true appeal of the digital authoritarian model is not its supposed benefits to citizens but its simplicity. It is cheap and easy to be a digital authoritarian.

To counter the spread of this model effectively, we must raise the cost while also offering a positive democratic vision in exchange. Autocrats have purchased their hold on power by spending billions of dollars to control what people can say, share, and access online.

While the United States and our allies cannot match these investments dollar for dollar, we must proportionally increase our efforts to make digital authoritarianism more difficult, more expensive, and less effective.

First, we need to increase our investments in internet freedom technologies to reduce the efficacy of repressive tools. People living under authoritarian regimes are our greatest ally in this cause, and we must ensure they have the tools to combat digital controls for themselves. This is why OTF supports technologies that counter even the most advanced forms of censorship and surveillance.

Second, we need to empower civil society coordination to bring it in line with the speed of authoritarian information sharing. In

many countries civil society organizations are working in isolation to identify and mitigate digital threats.

There is an urgent need for better coordination. Beyond the tangible benefits to those under attack, this coordination significantly increases the cost of authoritarian control.

And the private sector must engage as well. They are often excluded from important markets unless they make unreasonable accommodations that conflict with their stated values. It is in all our best interest to keep global markets open and fair without sacrificing our principles.

Members of the subcommittee, we must counter this challenge where it originates—in China, Iran, and Russia. We must also advocate for a better model where it is spreading.

The United States and its allies must advance a positive vision for a global internet that reinforces our democratic principles. We can show that it is possible to protect national security without undermining human rights and our democratic values.

The challenges posed by digital authoritarianism are daunting, and the path to a competing model is hard, but it is unquestionably worthwhile. If shown it is possible, most countries will opt for forms of digital governance that protect human rights.

But we need to lead the way. If we do not, China and Russia certainly will.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Cunningham follows:]

Prepared Statement of Ms. Laura Cunningham

Chairman Van Hollen, Ranking Member Romney, and distinguished Members of the Subcommittee, thank you for inviting me to testify today on the threat of digital authoritarianism and how we can ensure the global digital ecosystem reinforces our democratic principles.

Today two-thirds of the world's population—nearly 5.5 billion people—live in a country where the global internet is censored.

And this number is only increasing as authoritarian governments around the world are harnessing technological advances to increase the scale, scope, and efficiency of digital repression. But this is not merely a technical challenge. At its core, it is a normative contest to determine whether governments use technology to entrench authoritarian control or empower democratic freedoms.

ABOUT OTF AND INTERNET FREEDOM

The Open Technology Fund (OTF) was established over a decade ago—with bipartisan support and funding from Congress—in recognition of the dire consequences that unchecked digital authoritarianism poses to democratic principles, our national security, and human rights globally.

Today, OTF is a congressionally authorized non-profit funded through a grant from the U.S. Agency for Global Media. OTF's mission is to advance internet freedom in repressive environments by supporting the research, development, implementation, and maintenance of open source technologies that provide secure and uncensored access to the internet and counter attempts by authoritarian governments to control the internet and restrict freedom online.

OTF fulfills this mission by providing funding and support services to individuals and organizations around the world that are addressing threats to internet freedom with technical solutions. Broadly speaking, we invest in technologies that provide uncensored access to the internet to those living in information restrictive countries; and tools that protect at-risk populations, like journalists and their sources, from repressive authoritarian surveillance. For example:

• We provide anti-censorship technologies—specifically VPNs—to over 45 million people each month in countries where they would otherwise be cut off from the global internet, including China and Russia.

• We also support critical digital security technologies that enable journalists and human rights defenders working in repressive environments, like Myanmar and Cuba, to communicate, report, and share information safely.

• In addition, we invest in peer-to-peer and decentralized messaging tools that allow users to stay connected and access critical information during internet shutdowns, like those implemented by the Iranian government to suppress the anti-regime protests following the death of Mahsa Amini.

In total, over two billion people globally use OTF-supported technology daily, and more than two-thirds of all mobile users have OTF-incubated technology on their devices.

OTF's primary focus is on the human rights abuses that result from the application of repressive technologies. However, the threat I want to focus the Subcommittee's attention on today is far broader. The core challenge the United States must confront is a new authoritarian model that information control technologies have enabled, and not merely the technologies themselves.

Once considered politically extreme and technically implausible, digital authoritarianism has now been adopted worldwide as more and more governments are substituting repressive technical shortcuts for the hard work of good governance in a bid to control their populations in ways that were previously unimaginable.

Today, there is no longer a meaningful distinction between digital authoritarianism and authoritarianism of any other kind as online information control has become foundational to a newly possible form of illiberal governance. This is the greatest danger to democracy of our time, with profound implications for our democratic principles, national security, and global economic competitiveness.

ONLINE CENSORSHIP: BLOCKING FREE EXPRESSION & INDEPENDENT INFORMATION

Online censorship has become a central component to digital authoritarianism, facilitating easy and effective information control, which stifles dissent, eliminates government accountability, and obfuscates the truth. As a result, online censorship has become commonplace around the world.

According to Freedom House's Freedom on the Net Report, online censorship is at a historic high, with more governments censoring the internet than ever before. While many are familiar with the long history of internet censorship in the most extreme authoritarian contexts, like Russia and Iran, the reality is that online censorship is now normalized in dozens of countries around the world, including Belarus, Egypt, Ethiopia, Hungary, Kazakhstan, Myanmar, Nicaragua, Pakistan, Turkey, Uganda, Venezuela, Vietnam, and many more.

As online censorship has become more and more pervasive, autocrats are emboldened to utilize far more aggressive and blunt censorship techniques, including total internet shutdowns. Rather than narrowly blocking specific content and websites that a regime deems undesirable, authoritarians now regularly sever their citizens' connection to the internet entirely. For example, following the military coup in Myanmar, the junta implemented an internet shutdown, cutting millions of people off from the global internet in order to solidify political control. In fact, in 2023, 39 governments shut down the internet 283 times—a new record.

To further enhance their control, authoritarian regimes are leveraging AI to augment their censorship efforts to increase the scale, speed, and efficiency of online censorship. For example, the Russian government launched their own internet censorship and surveillance system called Oculus in February 2023. The new AI system automatically detects and blocks content the government considers "undesirable." And many other countries are following suit: at least 22 other countries now mandate or incentivize digital platforms to deploy machine learning to remove disfavored political, social, and religious speech at a rate and magnitude that was previously impossible for human censors to achieve.

With truthful information broadly blocked, digital authoritarians are able to perpetuate disinformation unchallenged. For example, Chinese media regularly reports that COVID originated from a U.S. lab; while in Russian media, the full-scale war in Ukraine is righteous and legitimate; and there are countless other examples. These narratives follow classic propaganda patterns designed to project domestic strength and unity, vilify perceived enemies; and establish a new, widely accepted "truth" that further cements political control.

Ultimately, online censorship erodes democracy by obscuring the truth, disempowering citizens, and creating extreme national echo chambers that create a more fractured and dangerous world.

MASS REAL-TIME SURVEILLANCE: SILENCING DISSENT AT HOME

Once only available to a small number of well-resourced autocrats, authoritarian governments are now pairing online censorship technologies with highly advanced surveillance tools. Distinct from more narrow forms of technical surveillance conducted within strictly prescribed limits and specific legal frameworks, leading digital authoritarians have normalized the unencumbered use of the world's most sophisticated surveillance tools to harass, intimidate, imprison, and stifle political opposition.

In the past 2 years, authoritarian governments—led by China and Russia—have taken extraordinary steps to expand their domestic surveillance capabilities. They have asserted authority to digitally collect personal information; engaged in widespread location tracking, tracing individuals' every movements; and pursued aggressive offline punishments for online activities.

Nowhere is the evolution in sophistication and scale of mass surveillance more evident than in China. The Uyghur community in Xinjiang experiences perhaps the most extreme version of surveillance imaginable. They are subject to constant monitoring from facial recognition-equipped cameras, mandatory use of surveillance software, police checkpoints, and informants. Police in Xinjiang use an app to collect massive amounts of personal information, which the app then uses to flag activities considered to be suspicious. The use of these tactics, and others like them, led directly to the imprisonment of as many as one million mostly ethnic Uyghur and Kazakh people.

Similarly in Russia, authorities are harnessing the power of biometric surveillance to target anyone critical of Vladimir Putin's regime and the full-scale war in Ukraine. More than 60 regions in the country have installed half a million cameras with facial recognition technology. A 2023 report revealed this technology played an important role in the arrests of hundreds of protesters in Russia.

As if these technical advancements and the resulting domestic repression were not alarming enough, research supported by OTF found that over the last decade, more than 110 countries purchased, imitated, or received training on information controls from China or Russia. For example, the Chinese telecom company ZTE is helping Venezuela develop a smart ID card that many fear will be used by the government as a powerful surveillance tool. The Serbian government also turned to a Chinese telecom company, acquiring a 1,000-camera-strong surveillance system from Huawei. And Huawei has built over 70 percent of the 4G networks on the African continent, raising concerns around surveillance and user privacy. Validating these fears, the Wall Street Journal revealed that Huawei technicians had helped the governments of Uganda and Zambia spy on political dissidents.

The near-universal reach of mass, domestic surveillance effectively contains and constrains billions of people worldwide. One of the more pernicious aspects is the extent to which the specter of surveillance, and very real fear of real world consequences, incentivizes a culture of self-censorship, further perpetuating unchecked authoritarian control.

With such powerful tools at their disposal, few authoritarians are willing to stop at their own national borders. Increasingly autocrats are attempting to extend their reach, and impose globally the same level of absolute control that they wield within their national boundaries.

COMMERCIAL SPYWARE: POWERING TRANSNATIONAL REPRESSION

The impunity with which authoritarians are able to surveil their citizens at home and abroad has been supercharged by the ready availability of commercial spyware products. These technologies have been used disproportionately to intimidate and harass journalists, human rights defenders, and political opposition figures. In the last decade, at least 75 countries—nearly 40 percent of all nations—have acquired commercial spyware, giving rise to a lucrative mercenary industry, now worth billions, that is flourishing despite U.S. import restrictions and sanctions against some of the known actors in this space.

Today, any government with an interest in surveilling its citizens at home and abroad can easily acquire the tools necessary to conduct near real-time mass surveillance as a result of off-the-shelf, enterprise solutions to any malicious surveillance need.

Perhaps the most highly publicized of these tools is Pegasus, the chief product sold by the NSO Group, which has been used largely by governments to target thousands of human rights activists, journalists, politicians, and government officials across 50 countries. Public reporting has found that from 2016 to 2021, at least 180 journalists were selected for potential targeting in 20 countries, including those with limited or declining media freedom. Our colleagues at Radio Free Europe/Radio Lib-

erty in Azerbaijan and Armenia are among these. Infamously, family members of Jamal Khashoggi were targeted before and after his murder by Saudi operatives; and separately, as were members of the UK Prime Minister's Office.

The NSO Group is only one actor in the surveillance industry ecosystem, yet has caused tremendous, specific harm. And there are others, multiplying at a rapid pace, whose products are wielded to silence and control. The Russian Federal Security Service is reported to have used COLDRIVER in an extensive campaign against Russian and Belarusian non-profit organizations active abroad, Russian independent media in exile, and at least one former U.S. Ambassador. Similarly, the government of Egypt deployed Intellexa's Predator spyware to surveil a former political opposition figure living in Turkey and an exiled journalist. Predator is also known to have targeted, although not necessarily infected, members of the U.S. Congress including Congressman Michael McCaul, the Chairman of the House Foreign Affairs Committee.

What is particularly striking about each of these examples is the audacity with which governments targeted individuals outside their borders regardless of victims' nationality. This element is the true autocratic innovation inherent in commercial spyware, which has accelerated transnational repression, making it too straightforward and mainstream.

RECOMMENDATIONS

Authoritarian use of technology could convince some that these tools are inherently oppressive, but nothing could be farther from the truth. It is crucial to remember—as this Subcommittee knows well—that the internet offers extraordinary potential for global connection, inclusive democratic participation, and economic growth at a speed and on a scale unprecedented in human history. Digital technologies fuel learning, improve healthcare, drive scientific and economic development, and enhance government services. While authoritarians would like us to believe otherwise, the reality is that a free and open internet meaningfully improves the lives of billions of citizens worldwide.

It is clear that the true appeal of the digital authoritarian model is not its supposed benefits to citizens, but its simplicity: it boasts a novel tech stack; provides compelling solutions to short-term governance problems; and is increasingly accepted as legitimate. In short, it is cheap and easy to become a digital authoritarian.

To counter its spread effectively, we must raise the costs of digital authoritarianism while offering a positive, democratic vision in exchange. This will require action by multiple stakeholders.

RAISE THE COST OF DIGITAL AUTHORITARIANISM

Digital authoritarians have functionally purchased their hold on power by spending billions of dollars to control what billions of people can say, share, and access online. And for the most part, they have gotten their money's worth. While the United States and its allies cannot match autocratic investment dollar for dollar, we must proportionally increase our efforts to make digital authoritarianism more difficult, more expensive, and less effective.

First, we need to increase our investments in internet freedom technologies to reduce the efficacy of repressive tools. People living under digital authoritarian regimes are our greatest ally in this cause, and we must ensure they have tools and technologies to counter the worst effects of authoritarian digital controls for themselves. This is why OTF supports tools that mitigate the effects of even the most advanced control technologies. When Iran cuts off access to the internet to stifle protests and silence critics, we provide shutdown resistant communications tools to keep people connected. When Belarus attempts to surveil journalists, we can keep their communications with their sources safe. When Russia censors objective reporting on the war in Ukraine, we can unblock independent news sites for tens of millions of people.

Second, we need to empower civil society coordination to bring it in line with the speed of authoritarian information sharing in order to increase the cost of digital authoritarianism.

Digital repression is now "plug and play," and even comes with great customer service. Through both authoritarian information sharing and a robust market for commercial surveillance tools, governments looking for easier answers find them in this model. And the effects on those they govern are tragic.

In many countries, civil society organizations are working individually in isolation to identify and counter digital threats to their organizations and communities. Few have the resources or expertise to keep up with the pace or sophistication of new surveillance threats emerging from globally connected authoritarians. There is an

urgent need for coordination among civil society organizations to collect, analyze, and ultimately mitigate digital threats and attacks. OTF is already investing in such coordination.

Beyond the tangible benefits to those under attack, this coordination makes more costly digital authoritarians' means of control. When an authoritarian purchases an expensive digital exploit it will prove effective for only a matter of days rather than for years on end.

STRENGTHEN THE DEMOCRATIC MODEL

While we must counter digital authoritarianism where it originates—in China, Iran, Russia—we must also advocate for a better model where it is spreading, in many cases to weakly institutionalized states whose populations will be materially affected by their governments' choice of governance technologies.

The United States and its allies should advance a positive vision of a global internet that reinforces our democratic principles. In order to be successful in this endeavor, we must show that it is possible to protect national security and combat crime without undermining human rights and our democratic values.

While technologies themselves are generally value neutral, their design, deployment, and application rarely are. In many cases, states are confronted with legitimate governance challenges that digital authoritarian models solve for leaders who are unconcerned with the human rights cost. We must demonstrate that there is a better way to solve these problems that harnesses the positive power of newly emergent technologies within a rights-preserving framework.

The private sector will also be vital to realizing this new model. As U.S. companies have been collateral damage in authoritarians' quest for control, they share common cause. Digital authoritarianism excludes the U.S. private technology sector from important markets unless they are willing to make unreasonable accommodations to authoritarian demands that conflict with many of these companies' stated values. The private sector is often left with the choice between their bottom line and respect for democratic values and human rights. We must strive to keep global markets open and fair without sacrificing principles.

This is a shared challenge, and we need shared solutions. The public sector, private sector, and civil society benefit from a free and open global internet. We must collectively defend it.

CONCLUSION

The challenges posed by digital authoritarianism are daunting and the path to a competing model is hard. But it is unquestionably worthwhile. Given a choice, many countries will opt for free, human rights-respecting digital governance approaches—if they are shown that this is possible. But we need to lead the way. If we don't, China and Russia certainly will.

Thank you and I look forward to your questions.

Senator VAN HOLLEN. Mr. Kaye.

STATEMENT OF DAVID KAYE, CLINICAL PROFESSOR OF LAW, UNIVERSITY OF CALIFORNIA IRVINE, IRVINE, CALIFORNIA

Mr. KAYE. Chairman Van Hollen, Ranking Member Romney, distinguished members of the subcommittee, thank you for the invitation to speak before you today.

My written testimony explores how authoritarianism and global competition over cyberspace are putting extraordinary strains on human rights, democracy, and U.S. national security, focusing on commercial mercenary spyware.

Here I will limit myself to the following summary points. First, the commercial spyware threat is real and deeply intrusive. With sophisticated exploits of device vulnerabilities, governments can buy a service that gives them access to text messages and calls, photos and files, contacts and locations—everything on your device and in real time.

Proponents pitch spyware as necessary to control terrorism and crime. Yet, report after report has demonstrated that spyware is

used to target the pillars of democratic society—journalists, opposition figures, human rights activists, even government officials and embassy personnel.

Israel's NSO Group may be most known for its widely reported Pegasus spyware, but a shadowy industry is manufacturing, marketing, selling, and servicing mercenary spyware. Members of Congress and U.S. Government personnel have been in spyware's crosshairs. We are careening toward a highly destabilized world where no one is safe from cheap, sophisticated spyware.

So what is to be done about it? In 2019, in a report to the U.N. Human Rights Council, I argued for limits on the uses of such surveillance technologies to manifestly lawful ones only, subjected to the strictest sorts of oversight and authorization with private sector participation in the spyware market conditioned on human rights due diligence and a track record of compliance with human rights norms.

At the time I urged a moratorium on the industry pending the imposition of enforceable regulations and tighter export controls. Since then Congress has enacted laws with a clear understanding that foreign commercial spyware poses national security and human rights threats.

U.S. agencies have sanctioned spyware companies for, quote, "activities that are contrary to the national security or foreign policy interests of the United States," end quote.

President Biden promulgated Executive Order 14093 constraining spyware's use and condemning its interference with fundamental rights and U.S. national security. And the United States has led a growing coalition of 21 governments to pursue domestic and international controls on spyware. These and other efforts may in fact be having an impact with emerging evidence that the cost of undermining human rights and U.S. national security is, indeed, high.

Still, the threat persists. The demand remains. AI will indeed infuse the industry with an ever deepening power to interfere with democratic life. This subcommittee should thus encourage the development of global norms to counter it.

Congress could, for example, codify the rules of Executive Order 14093, and it could go further. It could explore ways to limit the foreign sovereign immunity barrier in state hacking cases and enable remedies to spyware victims in U.S. courts.

It could explore conditioning U.S. cooperation with other governments pending implementation of their commitments to prevent the export of spyware to end users likely to use it for malicious activity.

It could even condition assistance to governments on their commitment to demonstrate that rule of law and human rights standards apply to their use of commercial spyware.

Congress could also have a near term impact in a related area. The U.N. General Assembly will consider adoption of a new cybercrime convention this fall. The convention and initiative pressed originally by Russia sends a contrary message on targeted surveillance at the very moment that the United States is pushing for constraint.

The Freedom Online Coalition Advisory Network has said it would enable and legitimize serious human rights violations due to multiple flaws and lack of safeguards and fundamental rights protections.

Senate expressions of concern could focus attention on the harm the convention would do and urge abstention or a no vote. In short, democracies need not be sitting ducks. They have the tools to counter the rise of global authoritarian in cyberspace.

The U.S. has begun to deploy those tools and to counter spyware's lawlessness, and I urge the subcommittee to continue its critical support in the legal fight for freedom online.

Thank you very much.

[The prepared statement of Mr. Kaye follows:]

Prepared Statement of Mr. David Kaye

Chairman Van Hollen, Ranking Member Romney, Members of the Subcommittee:

Thank you very much for the invitation to appear before you today. My name is David Kaye. I am a law professor at the University of California, Irvine, School of Law, where I conduct research and teach courses in public international law, international human rights and humanitarian law, freedom of expression, and law and technology, and I direct the Law School's International Justice Clinic. I also serve as the U.S. Member of the European Commission for Democracy Through Law, the Venice Commission. From 2014 to 2020 I served as the United Nations (UN) Special Rapporteur on freedom of opinion of opinion and expression, and from 2020 to earlier this year I was the independent chair of the Board of the Global Network Initiative.

The Subcommittee has an opportunity to help develop national and global standards to control, counter and sanction abuse of the most intrusive technologies of the digital age, and I thank you for taking on this essential task for human rights and democracies worldwide.

OVERVIEW: AUTHORITARIANISM AND THE THREAT TO "CYBERSPACE"

Authoritarianism and global competition over the future of "cyberspace" are putting extraordinary strains on human rights, democracy and U.S. national security. Several states, led by China and Russia, are seeking to undermine the international human rights framework that is at the foundation of global democracy. They seek to redefine the very norms that have been at the center of the global value system since Eleanor Roosevelt led the negotiation of the Universal Declaration of Human Rights over seventy-five years ago. They aim to impose the state's authority over the internet in ways that are fundamentally at odds with the idea that digital space should strengthen civil society and promote freedom of expression, access to information and public participation in the life and politics of one's nation. They wage this effort in the major global forums of the day, including but not limited to the U.N. Human Rights Council and the negotiations for a Global Digital Compact and U.N. Cybercrime Convention.

As grave as the normative challenge in cyberspace is, it admittedly has an abstract quality to it. Not so on the technical and operational side, where the threats are tangible and the victims suffer serious harms. The old tactics, of course, have not disappeared. Contemporary authoritarian governments censor and criminalize criticism and dissent; intimidate, harass, jail and sometimes torture and kill journalists, human rights activists, and opposition figures; repress civil society organizations and weaponize the law and the concept of sovereignty to limit NGO activity.

The digital age has enabled states to turbocharge these tactics—and to do so at an ever decreasing cost. Why censor a mere newspaper or jam a radio transmission when you can order the internet to be shut down, or block a website or an app? Why engage in transparent public diplomacy when you can use disinformation and propaganda on social media? Why pursue the tedious work of physical surveillance or wiretapping when you can buy off-the-shelf technology to sweep up all of a person's digital footprint without their knowledge?

In my testimony, I will focus on one of these representative digital threats, commercial mercenary spyware, in part because it poses such severe and demonstrated risks not only to human rights and democracy but to national security. Congress and the Biden administration have taken world-leading steps to address the threat of commercial spyware, but there is much more to do, and that is why this hearing

is so important. Therefore, I will first provide an overview of the nature of the threats posed by spyware to democracy, human rights and national security. I will then review steps that the United States and some within the international community are taking to address these grave threats. I will conclude with some broader remarks about the global threats and highlight steps the Senate should take to push an online rights-and-security agenda forward.

I. SPYWARE'S THREATS TO HUMAN RIGHTS AND NATIONAL SECURITY

In 2019, as U.N. Special Rapporteur, I reported on what seemed then to be a rapidly emerging threat of targeted digital surveillance.[1] At the time, I noted a range of digital attacks perpetrated by governments, often using tools supplied from a largely unregulated private industry. The report identified a range of serious attacks against human rights defenders, journalists and those simply in dissent, including by use of computer interference, commercial spyware and other forms of mobile device hacking, social engineering and phishing operations, network surveillance, abusive uses of facial and affect recognition, cell phone interception through tools known as IMSI catchers, and deep packet inspection.

Even then, it had become clear that commercial spyware was emerging as one of the gravest of all of these digital threats. Practically at the very moment that our lives had become persistently online, centered on devices that we all carry with us and that eventually lead back to the most personal details of our lives, careers, connections and opinions, an industry had arisen to intrude into our private spaces. It is an industry that develops exploits that take advantage of vulnerabilities in our devices, in turn providing governments with advanced capabilities allowing them to discretely, sometimes without even the requirement that a target click on a link or answer a call or message, install spyware on a mobile device, typically a smartphone. We can all imagine ourselves in the position of a victim: Spyware would give the attacker access to your text messages and phone calls, your photos and files, your contacts—indeed, everything on your device would be available to the attacker. Not only that, the possibility of microphone and camera access converts a device into "a bug in your pocket," as one analyst memorably put it.[2] The potential for abuse is obvious when made available without constraint to client governments unbound by the kinds of fundamental rules of law expressed in international human rights law or the U.S. Constitution's Fourth Amendment.

Beginning over a dozen years ago, The Citizen Lab at the Munk School of Global Affairs and Public Policy at the University of Toronto began to put out report after report detailing uses of spyware against journalists, opposition figures, human rights defenders, and researchers, among others.[3] Since then, it has been joined by

---

[1] Report of the Special Rapporteur on Freedom of Opinion and Expression: Surveillance and Human Rights, A/HRC/41/35, May 28, 2019, available at https://www.ohchr.org/en/documents/thematic-reports/ahrc4135-surveillance-and-human-rights-report-special-rapporteur.

[2] Written testimony of John Scott-Railton, Senior Researcher, the Citizen Lab, before the 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.

[3] See, e.g., Citizen Lab, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuous Proliferation," October 15, 2015, available at https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/; Citizen Lab, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender," August 24, 2016, available at https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; Citizen Lab, "HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," September 18, 2018, available at https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/; Citizen Lab, "Pegasus vs. Predator Dissident's Doubly Infected iPhone Reveals Cytrox Mercenary Spyware," December 16, 2021, available at https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/; Citizen Lab, "GeckoSpy: Pegasus Spyware Used against Thailand's Pro-Democracy Movement," July 17, 2022, available at https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/; Citizen Lab, "PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions," September 22, 2023, available at https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-Presidential-ambitions/.

other non-government organizations, especially Amnesty Tech[4] and Access Now,[5] which have together demonstrated the use of spyware on every continent against the pillars of democratic life.

Given commercial spyware's extraordinary level of intrusiveness, the risks to fundamental rights are correspondingly severe. Human rights law—such as the International Covenant on Civil and Political Rights, which the United States ratified in 1992—protects individual rights to privacy, religious belief and conscience, opinion and expression. These rights are foundational to democratic societies, and spyware directly interferes with them. It causes individuals to doubt the privacy of their communications and opinions, strategically designed to cause people to question their intentions to engage in private and public discourse. Just days ago, one victim put the feeling this way:

"The devastation I felt after discovering that the security agents who had tortured me in Bahrain had successfully hacked my phone and violated my privacy on British soil was overwhelming. I spent countless sleepless nights fearing the potential harm to those who had entrusted me with their sensitive information."[6]

As another put it, "'There were a lot of personal conversations which are not meant for anybody's ears. . . . For me, it was clearly a very dirty interference in my private life.'"[7] Galina Timchenko, co-founder, CEO, and publisher of the Russian-language media outlet Meduza, targeted with Pegasus spyware, said,

"The only thing that I am really worried about is that those people whose devices were infected with Pegasus also sometimes became targets of physical attacks. So now I have to look over my shoulder. And if this was Russia, where any citizen can be persecuted for cooperating with 'undesirable organizations,' then my main fear is how can I protect other people, our partners? Because those who targeted me now have all of my contact list."[8]

The mere potential that spyware could be used against them causes victims—and would-be victims who do not know if they have been subjected to spyware—to question the safety of speaking their mind, risking a spiral of intimidation and self-censorship that eats at the foundations of democratic debate. I hardly need say this to legislators, but for democratic societies, that withdrawal can be fatal, particularly when the targets of such intrusions are those we depend upon to inform our public life and debate, such as human rights defenders, journalists and their sources, civil servants, and elected leaders like you.

As harmful as spyware is to human rights and democracy, evidence shows that spyware is also a national security threat. The Pegasus Project, a multinational journalistic reporting endeavor, suggested potential targets at the highest levels of democratic governments.[9] One investigative project reported that Vietnamese government agents sought to infect the phones of Members of Congress with Predator spyware, produced by the Intellexa Group, a group on the U.S. sanctioned entity

---

[4] See, e.g., Amnesty Tech, "Forensic Methodology Report: How to catch NSO Group's Pegasus," July 18, 2021, available at https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/; Amnesty Tech, "Dominican Republic: Pegasus spyware discovered on prominent journalist's phone," May 2, 2023, available at https://www.amnesty.org/en/latest/news/2023/05/dominican-republic-pegasus-spyware-journalists-phone/ ; Amnesty Tech, "Global: A Web of Surveillance—Unravelling a murky network of spyware exports to Indonesia," May 2, 2024, available at https://www.amnesty.org/en/latest/news/2024/05/unravelling-a-murky-network-of-spyware-exports-to-indonesia/.

[5] See, e.g., Access Now, "Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict," May 25, 2023, available at https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/; Access Now, "Hacking Meduza: Pegasus spyware used to target Putin's critic," September 13, 2023, available at https://www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic/; Access Now, "New spyware attacks exposed: civil society targeted in Jordan," February 1, 2024; Access Now, "Exiled, then spied on: Civil society in Latvia, Lithuania, and Poland targeted with Pegasus spyware," May 30, 2024, available at https://www.accessnow.org/publication/civil-society-in-exile-pegasus/.

[6] See Global Legal Action Network, "New Criminal Complaint Over Pegasus Spyware Hacking of journalists and activists in the UK", September 19, 2024, available at https://www.glanlaw.org/single-post/new-criminal-complaint-over-pegasus-spyware-hacking-of-journalists-and-activists-in-the-uk.

[7] Suzanne Smalley and Daryna Antoniuk, "The inside view of spyware's 'dirty interference,' from two recent Pegasus victims," THE RECORD, June 25, 2024, available at https://therecord.media/pegasus-spyware-victims-sannikov-erlikh.

[8] Natalia Krapiva, "Hacking Meduza: Pegasus spyware used to target Putin's critic, ACCESS NOW, September 13, 2023, available at https://www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic/.

[9] See, e.g., THE GUARDIAN, The Pegasus Project, available at https://www.theguardian.com/news/series/pegasus-project.

list.[10] At the time that the Biden Administration announced its Executive Order addressing the spyware threat last year, it noted that "U.S. Government personnel overseas have been targeted by commercial spyware."[11]

The reporting from NGO's and journalists around the world indicated that one company, the Israel-based NSO Group, was responsible for many of the most egregious instances of spyware's abuse that have come to light. The NSO Group is part of a broader, opaque industry manufacturing, marketing, selling, transferring, and servicing mercenary spyware. The industry pitches its products as necessary for the control of terrorism and crime. Yet the industry has offered little proof of this claim of necessity, while the widespread exposure that commercial spyware has been used for state-on-state espionage belies the claims of necessity. On top of this lack of proof, there are troublingly few controls on the global proliferation and use of spyware. Even as the world became aware of the extraordinary abuses carried out using mercenary spyware, regulation and control, at national and international levels, lagged far behind.

In my 2019 U.N. report, I argued that it was imperative that governments limit the uses of spyware technologies to lawful ones only, subjected to the strictest sorts of oversight and authorization, and that they condition private sector participation in the spyware market—from research and development to marketing, sale, transfer and maintenance—on human rights due diligence and a track-record of compliance with human rights norms. I argued then that members of the industry should adopt and implement the U.N. Guiding Principles on Business and Human Rights, which establish a framework for companies to prevent or mitigate the human rights harms they cause,[12] but that responsibility, particularly in the context of such severe human rights impacts, must be overseen by public authorities and enforced by domestic and international law. At the time, I urged a moratorium on the industry, pending the imposition of enforceable rules, and while other U.N. rapporteurs and NGO's joined that call, civil society experts have developed a range of legal responses to spyware that include arguments for regulation and tighter export controls, while some even argue for a ban given the severity of the harms caused by spyware.

What is most remarkable, perhaps, apart from the persistent evidence of human rights and national security harms, is how quickly the industry rose and how rapidly its tools have been used against so many types of targets. Spyware's relative cheapness has enabled it to proliferate, destabilizing not only civil society but diplomatic and security sectors. It is easy to see how spyware's impact undermines fundamental democratic practice. But at the same time we are not safer when any government with access to spyware can hack, for instance, U.S. or NATO officials' phones. And yet this is the world to which we seem to be careening.

One last point connects the spyware industry and the global threat landscape. The companies that make mercenary spyware often emphasize how much control they have over the technology when asked about proliferation risk. Yet recent work by Google's Threat Analysis Group has shown that Russian hackers obtained and used exploits, the building block of the spyware trade, previously used by NSO Group and Intellexa.[13] In this sense, the spyware industry is directly helping to fuel the capabilities of U.S. adversaries. The threats are that sophisticated, matching the persistence and intrusiveness typically only seen from states like Russia and China. This concerning nexus suggests that, at minimum, there is cross pollination between these industries, and that the mercenary spyware industry may be helping to buoy the exploit marketplace.

---

[10] Tim Starks, "The trail of Predator spyware leads to targets in Congress," THE WASHINGTON POST, October 10, 2023, available at https://www.washingtonpost.com/politics/2023/10/10/trail-predator-spyware-leads-targets-congress/.

[11] FACT SHEET: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security, March 27, 2023, available at https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/.

[12] United Nations, GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS (2011), available at https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

[13] Google Threat Analysis Group, "State-backed attackers and commercial surveillance vendors repeatedly use the same exploits," August 29, 2024, available at https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/.

II. U.S. ACTIONS TO ADDRESS THE SPYWARE THREAT

The commercial spyware industry's intersecting threats to human rights and democracy and U.S. national security led the U.S. Government to act. In 2021, in the National Defense Authorization Act for 2022, Congress required the Secretary of State to prepare a list of contractors that have "knowingly assisted or facilitated a cyberattack or conducted surveillance" against the United States or against:

" . . . [i]ndividuals, including activists, journalists, opposition politicians, or other individuals for the purposes of suppressing dissent or intimidating critics, on behalf of a country included in the annual country reports on human rights practices of the Department for systematic acts of political repression, including arbitrary arrest or detention, torture, extrajudicial or politically motivated killing, or other gross violations of human rights." 22 USC § 2679e(a)(2).

In 2022, as part of the National Defense Authorization Act for 2023, Congress required U.S. intelligence agencies to provide annual reports assessing counter-intelligence threats "and other risks to national security" that "foreign commercial spyware" poses to the United States.[14] It further authorized the Director of National Intelligence to prohibit intelligence agencies from "entering into any contract or other agreement for any purpose with a company that has acquired, in whole or in part, any foreign commercial spyware."

The Biden administration, for its part, has taken steps to address the spyware problem consistent with U.S. law. In 2021, the Bureau of Industry and Security (BIS) of the Commerce Department added several companies, including the spyware companies NSO Group and Candiru, to the list of entities "engaging in activities that are contrary to the national security or foreign policy interests of the United States."[15] Specifically it noted,

"NSO Group and Candiru (Israel) were added to the Entity List based on evidence that these entities developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers. These tools have also enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent. Such practices threaten the rules-based international order."[16]

In February of this year, BIS added Sandvine, a Canadian-incorporated company whose "technology has been misused to inject commercial spyware into the devices of perceived critics and dissidents."[17] In July of this year, BIS added four other entities to the Entity List for "trafficking in cyber exploits used to gain access to information systems, threatening the privacy and security of individuals and organizations worldwide."[18]

The Department of Treasury's Office of Foreign Assets Control (OFAC) has identified several commercial spyware entities and persons associated with them as Specially Designated Nationals. As a result of such designations, all property and interests in property of such individuals or entities in the United States are blocked. Such spyware vendors as NSO Group and Intellexa have been designated under the program. For example, just this March, OFAC designated Intellexa and its key personnel "for their role in developing, operating, and distributing commercial spyware technology used to target Americans, including U.S. Government officials, journalists, and policy experts."[19]

In perhaps the most important example of the administration's recognition of the spyware threat to national security and foreign policy interests, in 2023 President

---

[14] Public Law 117–263 (50 USC § 3232a) (2022).

[15] Department of Commerce, "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities," November 3, 2021, available at https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

[16] Id.

[17] Department of State, "The United States Adds Sandvine to the Entity List for Enabling Human Rights Abuses," February 28, 2024, available at https://www.state.gov/the-united-states-adds-sandvine-to-the-entity-list-for-enabling-human-rights-abuses/.

[18] Department of Commerce, "Commerce Adds Four Entities to Entity List for Trafficking in Cyber Exploits," July 18, 2023, available at https://www.bis.gov/press-release/commerce-adds-four-entities-entity-list-trafficking-cyber-exploits-0.

[19] U.S. Department of Treasury, "Press Release: Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium," March 5, 2024, available at https://home.treasury.gov/news/press-releases/jy2155.

Biden promulgated Executive Order 14093.[20] EO 14093 identifies a number of U.S. national interests, including the protection of "democracy, civil rights, and civil liberties." It condemns the use of commercial spyware to interfere with fundamental human rights, the rule of law and U.S. national security. As such, the order prohibits any Federal agency or department from making operational use of commercial spyware when they determine inter alia "that the commercial spyware poses significant risks of improper use by a foreign government or foreign person."[21] The order further articulates the bases upon which an agency could make such a determination, including uses in violation of international human rights law.[22]

In a demonstration of the emerging whole-of-government approach to spyware, moreover, acting under Section 212(a)(3)(C) of the Immigration and Nationalization Act, the Department of State established a program in February 2024 to restrict the issuance of visas to persons:

"[b]elieved to have been involved in the misuse of commercial spyware, to target, arbitrarily or unlawfully surveil, harass, suppress, or intimidate individuals including journalists, activists, other persons perceived to be dissidents for their work, members of marginalized communities or vulnerable populations, or the family members of these targeted individuals".[23]

Importantly, the restrictions also apply to:

"individuals believed to facilitate or derive financial benefit from the misuse of commercial spyware . . . including but not limited to developing, directing, or operationally controlling companies that furnish technologies such as commercial spyware to governments, or those acting on behalf of governments, that engage in [the misuse of commercial spyware]."

In addition to official steps by Congress and the Biden administration, individual litigants are seeking to use U.S. law in order to hold accountable spyware vendors and states that use spyware transnationally. A pending lawsuit brought by Meta (WhatsApp) against the NSO Group in U.S. courts may provide guidance as to the strength of various existing legal bases for remedy.[24] Yet barriers to accountability are real. In a case involving the Ethiopian government's hacking of an Ethiopian-American activist's computer in Maryland, a Federal court ruled that the Foreign Sovereign Immunities Act (FSIA) barred the action, an indication that changes to the FSIA may be required to provide a further measure of action against those governments that use spyware as a tool of transnational repression.[25] Yet while these lawsuits are important examples of how cases may be brought, the global nature of the issue and jurisdictional hurdles make it hard for victims to hold companies accountable. This was the case, for instance, when the NSO Group's Pegasus spyware was used to hack journalists in El Salvador[26] (at least one of whom is a U.S. citizen[27]). Victims are seeking to hold NSO Group accountable in U.S. court.[28]

The United States is not alone among governments in having grave concerns about the commercial spyware threat. Poland has launched a major investigation into the previous government's use of Pegasus spyware against journalists and opposition figures, among others.[29] The European Parliament established a committee

---

[20] The White House, Executive Order on Prohibition on Use by the U.S. Government of Commercial Spyware that Poses Risks to National Security, March 27, 2023, available at https://www.whitehouse.gov/briefing-room/Presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/.

[21] EO 14093, Section 2(a).

[22] Id., Section 2(a)(ii)(A)(1).

[23] Secretary of State Antony Blinken, "Press Statement: Announcement of a Visa Restriction Policy to Promote Accountability for the Misuse of Commercial Spyware," February 5, 2024, available at https://www.state.gov/announcement-of-a-visa-restriction-policy-to-promote-accountability-for-the-misuse-of-commercial-spyware/.

[24] See, e.g., Jonathon Penney and Bruce Schneier, "Platforms, Encryption and the CFAA: The Case of WhatsApp v. NSO Group," 36 Berkeley Tech. L. Journal 469 (2021), available at https://btlj.org/wp-content/uploads/2022/03/0005-36-91-Schneier.pdf.

[25] See Doe v. Federal Democratic Republic of Ethiopia, 851 F.3d 7 (D.C. Cir. 2017), reh'g denied, 2017 U.S. App. LEXIS 10084 (D.C. Cir. June 6, 2017).

[26] The Citizen Lab, "Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware," January 12, 2022, available at https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/.

[27] Ronan Farrow, "A Hacked Newsroom Brings A Spyware Maker to U.S. Court," THE NEW YORKER, November 30, 2022, https://www.newyorker.com/news/news-desk/a-hacked-newsroom-brings-a-spyware-maker-to-us-court-pegasus.

[28] See Knight First Amendment Institute, Dada v. NSO Group, available at https://knightcolumbia.org/cases/dada-v-nso-group.

[29] Shaun Walker, "Poland launches inquiry into previous government's spyware use," THE GUARDIAN, April 1, 2024, available at https://www.theguardian.com/world/2024/apr/01/poland-launches-inquiry-into-previous-governments-spyware-use.

that, following extensive hearings, published a major report on the spyware threat in Europe, and the Parliament followed with several recommendations to European states.[30] Recognizing the global nature of the threat, and the resultant need for global solutions, the Biden administration has led a multilateral effort to counter spyware. In a Joint Statement issued on 30 March 2023, the United States and ten other states pledged to pursue "domestic and international controls" on spyware.[31] On the eve of this week's U.N. General Assembly, the State Department announced that additional states had joined the pledge, bringing to twenty-one the number of states signing up to counter spyware. That list now includes Australia, Austria, Canada, Costa Rica, Denmark, Estonia, Finland, France, Germany, Ireland, Japan, Lithuania, the Netherlands, New Zealand, Norway, Poland, Republic of Korea, Sweden, Switzerland, the United Kingdom, and the United States. The State Department is also setting aside funds to help low and middle income countries to develop better policies and oversight around spyware.[32]

These efforts may be having an impact on the spyware industry. Recently, the aforementioned Sandvine announced what appears to be a major transformation in its business, noting that, "In response to concerns regarding the misuse of our technology by foreign governments, we made a commitment to new ownership, leadership, and business strategy."[33] It has been suggested that, in light of the pressure from the United States and others, and the recognition of investors that association with threats to democracy and national security are bad for business, the spyware industry faces serious threat.[34]

III. A CONGRESSIONAL AGENDA TO COUNTER SPYWARE

The spyware threat is potentially at an inflection point. The United States has taken firm action against the commercial spyware industry, and twenty-one governments have committed to taking robust actions to address the threat, but the evidence of continuing threat persists. The demand for spyware products remains, especially by governments that lack any kind of commitment to rule of law and the protection of fundamental human rights. AI tools are likely to infuse the spyware industry with an ever-deepening power to interfere with the foundations of democratic life and to expose U.S. and allied government officials and employees to the serious risks causes by targeted surveillance. All of this is happening at a time when U.S. adversaries like Russia and China are seeking to redefine what human rights in cyberspace even means—to eliminate the well-established principle that human rights offline apply online just the same.

This Subcommittee has the power to encourage the development of global norms to counter the spyware threat, to promote human rights and democracy and to protect U.S. interests and national security. The Joint Statement on countering commercial spyware, mentioned above, contains a set of global commitments which Congress should support. A congressional agenda should include the following:

1. Congress could ensure that the rules of Executive Order 14093 are codified as statutory obligations of U.S. agencies. But it could also go beyond EO 14093. For instance, as noted above, victims face serious barriers when they seek to hold foreign states accountable for hacking that implicates them in the United States. Federal courts, for one thing, have adopted a narrow reading of the Foreign Sovereign Immunities Act. Congress could explore ways to make remedies available to such victims in U.S. courts.[35]

---

[30] See "European Parliament recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware," available at https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html.

[31] U.S. Department of State, "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware," September 22, 2024, available at https://www.state.gov/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/.

[32] U.S. Department of State, "New U.S.-led Actions Expand Global Commitments to Counter Commercial Spyware," September 22, 2024, available at https://www.state.gov/new-u-s-led-actions-expand-global-commitments-to-counter-commercial-spyware/

[33] See Sandvine, "Our Next Chapter as a Market Leader for Technology Solutions," September 19, 2024, available at https://www.businesswire.com/news/home/20240919441171/en/Sandvine-Our-Next-Chapter-as-a-Market-Leader-for-Technology-Solutions.

[34] See Omer Kabir, "Is Israeli spyware a dying sector?" CALCALIST, April 23, 2023, available at https://www.calcalistech.com/ctechnews/article/twcgg3tql.

[35] See Spencer Levitt and Andrea Cervantes, The Foreign Sovereign Immunities Act in the Age of Transnational Surveillance: Judicial Interpretation and Legislative Solutions, Report of the UC Irvine School of Law International Justice Clinic, August 21, 2023, available at https://

Continued

2. Congress could encourage other governments to join the global effort to constrain commercial spyware. Congressional support for EO 14093 would go a long way in this direction. But in the face of the increasing threat of spyware's proliferation, Congress could also adopt appropriate conditions on U.S. assistance to or cooperation with other governments on their commitments to prevent, consistent with the 2023 Joint Statement, the export of software, technology, and equipment to end-users likely to use them for malicious cyber activity; it could condition assistance to other governments on their commitment to adopt, implement and demonstrate, at a minimum, that rule of law and human rights standards apply to their use of commercial spyware technologies.

3. In keeping with the 2023 Joint Statement, Congress could also ensure that civil society groups have a place at the table in the national and global efforts to counter commercial spyware. It has been civil society organizations, after all, that have led the way in exposing the global threat of the commercial spyware industry. Further hearings like this one should bring the voices of security researchers, victims and their advocates to public awareness.

4. Congress could reinforce administration efforts to engage additional partner governments around the world to mitigate the misuse of commercial spyware and drive reform in this industry, including by encouraging industry and investment firms to implement the United Nations Guiding Principles on Business and Human Rights. A range of regulatory measures are available, drawing on experiences in other areas of international law, and Congress could play a meaningful role in pressing forward these ideas.[36]

In addition to spyware-specific steps, the congressional voice could have near-term impact in a related area. This Fall, the U.N. General Assembly is considering adoption of a new Cybercrime Convention. The draft Convention, originally an initiative pressed by the Russian Federation, may on its face appear to be a salutary effort to promote international cooperation. But its loose language and broad framing of "serious crimes" opens the door to a confusing international legal landscape that will almost certainly work to the detriment of human rights. The Freedom Online Coalition Advisory Network has called the draft "a far-reaching global criminal justice treaty that would enable and legitimize serious human rights violations due to multiple flaws and lack of safeguards and fundamental rights protections."[37] It has the potential to, at the very minimum, send a contrary message on government targeted surveillance at the very moment that the United States is pushing for constraint.[38] In advance of the U.N. General Assembly vote on the draft, Senate expressions of concern could focus U.S. Government and allied attention on the potential harm the convention could do and urge them to reject it.

In this way, my testimony returns to the beginning. Commercial mercenary spyware poses serious threats to cyberspace—but more specifically, to human rights and national security. It has become one of the key vectors for the furtherance of authoritarianism and repression in the digital age. But democracies need not be sitting ducks; they have the tools to counter the rise of global authoritarianism in cyberspace. The United States has begun to deploy rule of law in the face of spyware's lawlessness, and I urge the Subcommittee to continue its critical support of the legal fight for freedom online.

Senator VAN HOLLEN. And thank you.

Mr. Jaffer.

STATEMENT OF JAMIL N. JAFFER, FOUNDER AND EXECUTIVE DIRECTOR, NATIONAL SECURITY INSTITUTE, ARLINGTON, VIRGINIA

Mr. JAFFER. Chairman Van Hollen, Ranking Member Romney, thank you for holding this hearing.

---

bpb-us-e2.wpmucdn.com/sites.uci.edu/dist/2/4290/files/2023/08/The-Foreign-Sovereign-Immunities-Act-in-the-Age-of-Transnational-Surveillance.pdf.

[36] See, e.g., David Kaye and Sarah McKune, "The Scourge of Commercial Spyware—and How to Stop It," LAWFARE, August 25, 2023, available at https://www.lawfaremedia.org/article/the-scourge-of-commercial-spyware-and-how-to-stop-it.

[37] FOC Advisory Network Proactive Advice: U.N. Convention Against Cybercrime, September 16, 2024, available at https://freedomonlinecoalition.com/foc-advisory-network-proactive-advice-un-convention-against-cybercrime/.

[38] See Kate Robertson, "A Global Treaty to Fight Cybercrime—Without Combating Mercenary Spyware," LAWFARE, August 22, 2024, available at https://www.lawfaremedia.org/article/a-global-treaty-to-fight-cybercrime-without-combating-mercenary-spyware.

It is particularly important at a time, given the increasing drumbeat of threats that our Nation and our allies face from countries like China, Russia, Iran, and North Korea.

These countries are global repressors. They repress their own people at home, then they export that repression abroad, not just in their own regions but across the globe.

They engage in this export through a variety of activities, whether it is the sales of surveillance technology, their influence on online platforms, their cyber attacks and hacks against our nation and its allies, and the like.

They are engaged in a constant day in, day out attack on America, our allies, and free and open societies around the globe, and we must respond.

Chairman Van Hollen, you have led on some of these efforts with the BRINK Act and your efforts to speak out against the CCP and suppressive activities in Hong Kong and abroad.

Ranking Member Romney, you for decades have talked about the threat these countries pose to our nation and our allies. You spoke about Russia long before it was popular to speak about Russia and its repressive activities and long before they invaded in Ukraine not once, but twice. You have also talked about Iran and China's activities as well.

So the members of this committee and the leadership of this committee knows all too well the threats these countries pose. But their threats are not just obvious on the surface. They are surreptitious.

These countries spend hundreds of millions of dollars and billions of dollars investing in technology to embed that technology at the heart of our societies. Companies like Huawei and ZTE, supported by low and no interest loans from the Chinese government and grants from the Chinese government, embed their core network capabilities in networks around the globe.

By one measure, in Africa 70 percent of 4G networks are controlled by Huawei. Huawei sits at the heart of British telecom. It at the heart of telecommunications networks inside of our country in state and local networks.

Congress has taken action to combat this by providing funds to rip and replace some of this technology. More needs to be done and faster. Our allies are slowly getting on the board with this program, but are slow rolling it. Germany just this month announced it will slowly be removing Huawei technology from its networks but not till 2026.

And it is not just telecommunications capabilities. It is social media. Today, TikTok has 170 million Americans on its platform. It is the primary news source for Americans under the age of 30. A Chinese influenced platform is the primary news source for Americans under the age of 30.

And it is not that we do not know that TikTok uses its capabilities to message to Americans. We know that a variety ways. No. 1, we saw them push the Osama bin Laden narrative in the aftermath of the October 7 attacks.

We saw them suppress talk about their suppression of Muslim Uighurs and the genocide against Muslim Uighurs. We saw them suppress discussion about Tibet, and we saw them press this Con-

gress to have American young people call Senate and House offices to lobby against the TikTok legislation that was passed in the House and the Senate and eventually signed into law.

So we know that this platform is used for illicit activities by the CCP and its allies, and so it is so critical that we take action.

But it is not just cat videos and dancing videos on TikTok. It is also election messaging, and it is also the fact that the data that is collected on Americans using TikTok—the location of individuals, their voiceprints, who they communicate with—when combined with the mass amounts of data that we know China and other nations have stolen from Americans, including healthcare data, financial data, and the like, and all of that enhanced with AI technology to create targeting packages not just for intelligence collection but for covert messaging.

The same way that AI enhances the ability of our candidates to speak to the American electorate, it enhances the ability of China, Russia, Iran, and North Korea to speak to Americans as well.

And that is a very real danger, and so that is why it is so critical that we have this hearing today, that we hear about the capabilities that the Open Technology Fund is putting to work using congressionally appropriated funds to bring freedom to these nations.

But it is also important why we hear about commercial spyware and the like and what our adversaries are using as well, because it is important that we factor in that American investors are investing in these technologies and capabilities.

That is why it is important that Congress and the Administration partner with American investors who are willing to speak out against this and are willing to commit to not investing in adversary technology and to investing in American allied technology. We brought together a group of 20 investors. There are other groups as well in NATO and the Quad that are bringing these groups together as well.

And so I welcome the opportunity to be here today. Thank you for your time, and I look forward to any questions from the committee.

[The prepared statement of Mr. Jaffer follows:]

Prepared Statement of Mr. Jamil N. Jaffer [1]

INTRODUCTION

Chairman Van Hollen, Ranking Member Romney, and Members of the Subcommittee: thank you for inviting me here today to discuss the threats our nation

[1] Jamil N. Jaffer currently serves as Founder & Executive Director of the National Security Institute and the NSI Cyber & Tech Center and as an Assistant Professor of Law and Director of the National Security Law & Policy Program and the Cyber, Intelligence, and National Security LL.M. Program at the Antonin Scalia Law School at George Mason University. Mr. Jaffer is also a Venture Partner at Paladin Capital Group, a leading global multi-stage investor that identifies, supports and invests in innovative companies that develop promising, early stage technologies to address the critical cyber and advanced technological needs of both commercial and government customers. Mr. Jaffer serves on a variety of public and private boards of directors and advisory boards, including his recent appointment to serve as a member of the Cyber Safety Review Board at the Department of Homeland Security, an advisory board responsible for reviewing and assessing and significant cyber incidents affecting Federal civilian and non-Federal systems. Among other things, Mr. Jaffer previously served as Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee, Senior Counsel to the House Intelligence Committee, Associate Counsel to President George W. Bush in the White House, and Counsel to the Assistant Attorney General for National Security in the U.S. Department of Justice. Mr. Jaffer is testifying before this Subcommittee in his personal and individual capacity and is not testifying on behalf of any organization or entity, including but not limited to any current or

and our allies and partners face in the cyber domain, particularly from authoritarian regimes across the globe that seek to replace the United States as a key international leader.

I want to thank the Chairman and Ranking Member for holding this hearing, given the increasing drumbeat of threats that our nation and other free and open societies face from nations like China, Russia, Iran, and North Korea in the cyber domain. The regimes that control these nations form the core of a growing group of global repressors, nations that repress their own people at home, and then seek to extend that repression abroad, oftentimes not only within their own region but increasingly across the globe as well. Both of you have exhibited strong leadership on the issues at the core of this hearing, including ensuring that America leans forward and leads in the international realm, serving as the strongest ally to our friends and the fiercest foe to our adversaries. As you both well know, the promotion and protection of our national interests, including the protection of our citizens and the critical infrastructure they rely upon could not be more important in this era of expanding authoritarianism and rapidly evolving technologies. It is likewise critically important that, as a global leader, we also defend the democratic principles that undergird free and open societies globally, including the core concepts of free speech, economic liberty, and the rule of law. We must also guard vigilantly against repressive efforts by these regimes as they seek to undermine these democratic principles by depriving their own people and, increasingly, others around the globe, of access to economic freedom and the kind of basic rights that characterize free and open societies. [2]

Chairman Van Hollen, you are well known for your work in this space, including your bipartisan BRINK Act, which requires the imposition of sanctions on the foreign banks and companies that facilitate illegal financial transactions with North Korea, your advocacy to hold the Chinese Communist Party (CCP), which controls the People's Republic of China (PRC) with an iron fist, accountable for its attacks on freedom and democracy in Hong Kong and elsewhere, and your efforts to hold other authoritarian regimes accountable as they seek to expand their repression globally, including by targeting American elections. You also recognize the critical importance of ensuring that American remains competitive and that our critical edge is America's ability to rapidly innovate and that we must protect that innovation with a strong intellectual property system, so thank you for your leadership in those areas as well.

And Ranking Member Romney, you've long been a leading voice on American foreign policy, advocating for policies that promote our economic and national security and that of our allies and partners. You have been one of the primary leaders in our nation—whether during your time as Governor, as a candidate for President, and now in the Senate—that has always been clear-eyed and direct with the American people about the very real threat that we face from nations like Russia, China, Iran, and North Korea. Even when it was unpopular to do so, you have called out these nations for their bad behavior and highlighted the threat they pose to our Nation. Whether it was your successful effort to impose a diplomatic boycott during the 2022 Winter Olympics in Beijing or your calling out of Russia from the debate stage over a decade ago—presaging Russia's multiple invasions of Ukraine—no one can doubt where you stand on these issues and the critical importance of your leadership.

Mr. Chairman and Mr. Ranking Member, your bipartisan leadership and continued work together on this Subcommittee is critical to highlighting the many ways that these global repressors have sought to take advantage of our nation's free and open society—particularly in the cyber domain and with respect to emerging technologies—in order to gain political, economic, technological, and military advantage,

---

former employer or public or private entity. Mr. Jaffer would like to thank Keelin Wolfe, Ann Long, and Patrick Schmidt for their excellent research assistance with respect to this testimony.

[2] Significant portions of this testimony have also been drawn in whole or in part from prior testimony provided by Mr. Jaffer to the Senate Banking Committee in January 2024 and to the House Select Committee on the Chinese Communist Party in September 2024, as well as from an NSI Decision Memo entitled Addressing the National Security Threat of Chinese Technological Innovation by Jamil N. Jaffer published in July 2023. Citations to that testimony and paper and quotation marks for portions of this testimony drawn from those materials have been omitted, including where significant portions are excerpted verbatim. Links to both pieces of testimony can be found at the links provided below in footnote 2. In addition, Mr. Jaffer would like to thank Devlin Birnie, Jessica Jones, Harrison McClintock, and Alex Tokie for their excellent research and editing assistance with NSI Decision Memo which can be found at: https://nationalsecurity.gmu.edu/addressing-the-national-security-threat-of-chinese-technological-innovation-2/.

including in the context of the larger strategic competition taking place across the globe.

And as the members of the Subcommittee know all too well, China is the key economic and national security challenge facing our nation going forward, and its ongoing and expanding collaboration with other global repressors, including in the cyber domain and with respect to emerging technologies, is at the heart of these matters. I hope this hearing will offer us the opportunity to have a candid and frank discussion on these important matters.

I. THE OVERALL THREAT POSED BY A RISING CHINA AND ITS COLLABORATION WITH OTHER GLOBAL REPRESSORS IN THE CYBER DOMAIN AND ON EMERGING TECHNOLOGIES

As I testified last week before the House Select Committee on the Chinese Communist Party and earlier this year before the Senate Banking Committee, the threat of a rising China, under the leadership of the CCP, is the defining national security challenge facing the United States and our allies today.[3] Like other global repressors, the PRC, under the direction and control of the CCP, is a nation that not only oppresses its own people, but pushes that repression well beyond its borders, not just in the Indo-Pacific region, but across the globe as well. The genocide and crimes against humanity currently underway against Muslim Uyghurs in the Xinjiang region are but one example of the type of repressive activities that take place within the borders of CCP-controlled China, activities that also include the brutal repression of dissent and political, economic, and religious freedom in Hong Kong and Tibet.[4]

The global scale of the CCP's repression is vast, as can be seen in the PRC's near-constant drumbeat of military and economic threats against Taiwan,[5] its hostile actions and active threats toward other U.S. allies and partners globally,[6] its export of surveillance technologies and other repressive capabilities to authoritarian-leaning regimes worldwide,[7] its ongoing efforts to consolidate control over and withhold access to key critical minerals and strategic metals,[8] its extortion of dozens of coun-

---

[3] See Jamil N. Jaffer, Statement for the Record on How the CCP Uses the Law to Silence Critics and Enforce its Rule, U.S. House Select Committee on the Chinese Communist Party (Sept. 19, 2024), available online at <https://selectcommitteeontheccp.house.gov/committee-activity/hearings/how-ccp-uses-law-silence-critics-and-enforce-its-rule>; Jamil N. Jaffer, Statement for the Record on National Security Challenges: Outpacing China in Emerging Technology, U.S. Senate Committee on Banking, Housing, and Urban Affairs (Jan. 18, 2024), available online at <https://www.banking.senate.gov/imo/media/doc/jaffer__testimony.pdf>.

[4] See Michael R. Pompeo, Press Statement: Determination of the Secretary of State on Atrocities in Xinjiang, United States Department of State (Jan. 19, 2021), available online at <https://2017-2021.state.gov/determination-of-the-secretary-of-state-on-atrocities-in-xinjiang/> ("I have determined that since at least March 2017, the … PRC[], under the direction and control of the … CCP[], has committed crimes against humanity against the predominantly Muslim Uyghurs … in Xinjiang … .In addition … I have determined that the PRC, under the direction and control of the CCP, has committed genocide against the predominantly Muslim Uyghurs … in Xinjiang."); see also, e.g., United States Department of State, 2021 Country Reports on Human Rights Practices: China (Includes Hong Kong, Macau, and Tibet) (Apr. 12, 2022), available online at <https://www.state.gov/reports/2021-country-reports-on-human-rights-practices/china/>; United States Department of State, 2019 Country Reports on Human Rights Practices: China (Includes Hong Kong, Macau, and Tibet) (Mar. 2020), at pp. 89–131 (sections on Tibet and Hong Kong), available online at < https://www.state.gov/wp-content/uploads/2020/03/CHINA-INCLUSIVE-2019-HUMAN-RIGHTS-REPORT.pdf>.

[5] See, e.g., Nectar Gan, et al., China Starts "Punishment" Military Drills Around Taiwan Days After Island Swears in New Leader, CNN (May 23, 2024), available online at <https://edition.cnn.com/2024/05/22/asia/china-military-drills-taiwan-punishment-intl-hnk/index.html>.

[6] See, e.g., Matthew Olay, Threat From China Increasing, Air Force Official Says, DOD News (Sept. 16, 2024) available online at <https://www.defense.gov/News/News-Stories/Article/Article/3907669/threat-from-china-increasing-air-force-official-says/> ("[T]he Chinese Communist Party continues to heavily invest in capabilities, operational concepts and organizations that are specifically designed to defeat the United States and its allies' ability to project power … including weapons targeting U.S. land and sea assets like air bases and aircraft carriers."); Agnes Chang, et al., China's Risky Power Play in the South China Sea, N.Y. Times (Sept. 15, 2024), available online at <https://www.nytimes.com/interactive/2024/09/15/world/asia/south-china-sea-philippines.html>.

[7] See, e.g., Bulelani Jili, China's Surveillance Ecosystem and the Global Spread of its Tools, Issue Brief, Atlantic Council (Oct. 17, 2022), available online at <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/>; Sheena Chestnut Greitens, Dealing with Demand for China's Global Surveillance Exports, Brookings Inst. (Apr. 2024), available online at <https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200428_china_surveillance_greitens_v3.pdf>.

[8] See, e.g., Jared Cohen, et al., Resource Realism: The Geopolitics of Critical Mineral Supply Chains, Goldman Sachs Global Institute (Sept. 13, 2023), available online at <https://www.goldmansachs.com/insights/articles/resource-realism-the-geopolitics-of-critical-mineral-sup-

tries under the Belt and Road Initiative (BRI),[9] and its growing political, economic, and military relationships with other global repressors like Russia, Iran, and North Korea.[10]

But this litany of activities is only the beginning of the CCP's larger and more hidden effort to undermine our nation's security. The CCP has also long engaged in the broad-based theft of intellectual property from American and allied private sector companies to benefit its own economic base,[11] and the PRC's deep and expanding cyber infiltration of U.S. and allied critical infrastructure,[12] as well as its active installation of capabilities to hold such critical infrastructure at risk,[13] together pose a clear and present danger to our economic and national security. Likewise, the CCP has actively sought to recruit American and allied academics and intellectuals through its Thousand Talents Program[14] and has sought to shape minds

---

ply-chains> ("China now accounts for 85–90 percent of global REEs mine-to-metal refining . . . Likewise, China refines 68 percent of the world's cobalt, 65 percent of nickel, and 60 percent of lithium of the grade needed for electric vehicle batteries . . . Even though new discoveries of critical mineral reserves around the world continue to be made, China is still the top producer of 30 of the 50 critical minerals, in part because it mines at greater rates than other countries."); see id. ("In 2010, Beijing embargoed REE exports to Tokyo . . . [i]n 2020, China reportedly cut off exports of graphite to Sweden. Following up on the October 2022 US-led export controls on advanced computing and semiconductor products . . . Beijing announced its own export controls on gallium and germanium products to the United States in the summer of 2023.").

[9] See, e.g., Jamil N. Jaffer, Waking up to the Threat of the Chinese Communist Party: A Call to Action from Congress, The Hill (Feb. 28, 2023) (op-ed), available online at <https://thehill.com/opinion/national-security/3877095-waking-up-to-the-threat-of-the-chinese-communist-party-a-call-to-action-from-congress/> (arguing that "the CCP's Belt and Road Initiative, while masquerading as an economic development program, is actually a tool for massive economic theft and political coercion, designed to supply the Chinese government with resources and jobs for its population, while addicting developing nations to Chinese financing that they can't possibly repay"); see also Reid Standish, A Closer Look At China's Controversial Lending Practices Around The World, Radio Free Europe/Radio Liberty (Apr. 22, 2021), available online at <https://www.rferl.org/a/china-loans-around-the-world/31217468.html>; Anna Gelpern, et al., How China Lends: A Rare Look into 100 Debt Contracts with Foreign Governments, AidData, et al. (Mar. 2021) at 5–9, 34–45, available online at <https://www.cgdev.org/sites/default/files/how-china-lends-rare-look-100-debt-contracts-foreign-governments.pdf>.

[10] See, e.g., Max Bergmann, et al., Collaboration for a Price: Russian Military-Technical Cooperation with China, Iran, and North Korea, Center for Strategic International Studies (May 22, 2024), available online at <https://www.csis.org/analysis/collaboration-price-russian-military-technical-cooperation-china-iran-and-north-korea>; see also, e.g., Kimberly Donovan & Maia Nikoladze, The Axis of Evasion": Behind China's Oil Trade with Iran and Russia, The Atlantic Council (Mar. 28, 2024), available online at <https://www.atlanticcouncil.org/blogs/new-atlanticist/the-axis-of-evasion-behind-chinas-oil-trade-with-iran-and-russia/>.

[11] See, e.g., Jamil N. Jaffer, Addressing the National Security Threat of Chinese Technological Innovation, National Security Institute (Aug. 2023), at 1, available online at <https://nationalsecurity.gmu.edu/wp-content/uploads/2023/08/The-National-Security-Threat-of-Chinese-Technological-Innovation.pdf> ("Over time, the PRC came to rely upon the theft of U.S. intellectual property at industrial scale—referred to as the greatest transfer of wealth in modern human history—to create an entire industry of state-owned and state-influenced enterprises that, when combined today, generate a tremendous amount of the technology products and capabilities sold around the globe.") (internal citations omitted); Senator Carl Levin, Opening Statement of Chairman Carl Levin in Hearing to Receive Testimony on U.S. Strategic Command and U.S. Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2013 and the Future Years Defense Program, Senate Armed Services Committee (Mar. 27, 2012), at 3, available online at <https://www.armed-services.senate.gov/imo/media/doc/12-19%20-%203-27-12.pdf> ("General Alexander has stated that the relentless industrial espionage being waged against U.S. industry and Government chiefly by China constitute 'the largest transfer of wealth in history.'").

[12] See Cybersecurity and Infrastructure Security Agency, et al., PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, Alert Code: AA24-038A (Feb. 7. 2024), available online at <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.

[13] See id.; see also text accompanying n. 58 infra.

[14] See, e.g., Alison Snyder, China Talent Program Increased Young Scientists' Productivity, Study Says, Axios (Jan. 10, 2023), available online at <https://www.axios.com/2023/01/10/china-funding-young-scientists-productivity> (describing the Youth Thousand Talents Program (YTT), which offers more than 3,500 young researchers—both Chinese nationals and foreign-born scientists—funding and benefits to relocate full-time to China and also describing the Thousand Talents Program, a large effort that began in 2008 with the goal of recruiting top-caliber scientists to work with China; a part of that effort often allowed or even encouraged recruits to remain at their U.S. institutions while also working with the PRC); see also Emily S. Weinstein, Chinese Talent Program Tracker, Center for Security and Emerging Technology, Georgetown University (Nov. 2020), available online at <https://cset.georgetown.edu/publication/chinese-talent-program-tracker/> (noting that Chinese talent initiatives include 43 national-level programs and 200 talent programs at sub-national levels, numbers that are growing as the PRC "seeks

Continued

of students through its establishment of hundreds of Confucius Institutes across the globe. [15]

For the purposes of today's hearing, I'd like to focus on three area where the CCP seeks in particular to undermine U.S. interests in the cyber and emerging technologies domain: (1) the effort by China to embed its technologies around the globe in an effort to collect intelligence and influence political, economic, and military conditions; (2) the way the CCP is likely to exploit emerging technologies, like artificial intelligence, steal intellectual property, and use extortive efforts to undermine U.S. and allied leadership globally; and (3) the CCP's holding at risk of American and allied critical infrastructure in the cyber domain and to influence American and allied views. And I'd also like to highlight how China and other global repressors, like Russia, use international institutions, like the U.N. and various advisory committees and boards to also achieve their own ends. Finally, I'd like to focus on how we might usefully address some of these issues.

II. CHINA'S EFFORT TO EMBED ITS TECHNOLOGIES AROUND THE GLOBE IN AN EFFORT TO COLLECT INTELLIGENCE AND INFLUENCE POLITICAL, ECONOMIC, AND MILITARY CONDITIONS

China's ongoing and widespread effort to embed its technologies around the globe can be seen in numerous places across the globe. For example, the effort to embed Huawei and ZTE gear in the telecommunications networks of Western countries, including successful efforts in a number of U.S. States as well as at the heart of the British Telecom and other allied networks, and has been well-understood for over a decade. [16] Indeed, as far back as March 2015, as part of its Belt-and-Road Initiative, China announced a Digital Silk Road effort—ostensibly to provide aid to other nations to improve their telecom networks, AI capabilities, cloud computing, and surveillance technology, among other things—that puts Chinese national champions, like Huawei, deep in those networks. [17] Capabilities like these—which provide direct access into the core of the telecommunications networks—can be hugely valuable to our adversaries as a tool to collect massive amounts of information and intelligence, as well as to conduct actual offensive cyber attacks that can delete, destroy, or modify information and even take down entire networks. [18] Yet many nation-states have taken a while to understand the very real threat these capabilities pose to their na-

---

to retain, manage, and recruit talent globally"); Federal Bureau of Investigation, The China Threat—Chinese Talent Plans Encourage Trade Secret Theft, Economic Espionage, Federal Bureau of Investigation, available online at <https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans> (describing hundreds of talent programs that incentivize their members to "steal foreign technologies needed to advance China's national, military, and economic goals" including work on key programs like military technologies, nuclear energy, wind tunnel design, and advanced lasers, and noting that talent plan participants "enter into a contract with a Chinese university or company—often affiliated with the Chinese government—that usually requires them to [be] subject [] to Chinese laws, to share new technology developments or breakthroughs . . . [and to] recruit other experts into the program").

[15] Thomas Lum & Hannah Fischer, Confucius Institutes in the United States: Selected Issues, Congressional Research Service (May 2, 2023), available online at <https://crsreports.congress.gov/product/pdf/IF/IF11180>.

[16] See Chairman Mike Rogers & Ranking Member C.A. Dutch Ruppersberger, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, House Permanent Select Committee on Intelligence, U.S. House of Representatives (Oct. 8, 2012), available online at <https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf>; see also Andy Keiser & Bryan Smith, Chinese Telecommunications Companies Huawei and ZTE: Countering a Hostile Foreign Threat, National Security Institute (Jan. 24, 2019), available online at <https://nationalsecurity.gmu.edu/chinese-telecommunications/>.

[17] See Joshua Kurlantzick, Assessing China's Digital Silk Road Initiative, Council on Foreign Relations (Dec. 18, 2020), available online at <https://www.cfr.org/china-digital-silk-road/>; Chang Che and John Liu, 'De-Americanize': How China Is Remaking Its Chip Business, New York Times (May 11, 2023), available online at <https://www.nytimes.com/2023/05/11/technology/china-us-chip-controls.html>.

[18] See Rogers & Ruppersberger, Huawei and ZTE Investigative Report, supra n. 16 at 3 ("The ability to deny service or disrupt global systems allows a foreign entity the opportunity to exert pressure or control over critical infrastructure on which the country is dependent. The capacity to maliciously modify or steal information from government and corporate entities provides China access to expensive and time-consuming research and development that advances China's economic place in the world. Access to U.S. telecommunications infrastructure also allows China to engage in undetected espionage against the United States government and private sector interests . . . . Inserting malicious hardware or software implants into Chinese-manufactured telecommunications components and systems headed for U.S. customers could allow Beijing to shut down or degrade critical national security systems in a time of crisis or war. Malicious implants in the components of critical infrastructure, such as power grids or financial networks, would also be a tremendous weapon in China's arsenal.").

tional security and some continue to install these systems at the heart of their networks.[19] Indeed, according to one source, as of 2 years ago, "Huawei and its components comprise almost 70 percent of the total 4G networks across the [African] continent."[20]

Likewise, Congress and two successive Administrations have highlighted the very real threat that social media applications, like TikTok, pose to our national security.[21] This national security threat is described in extensive detail in an amicus brief that was filed on my behalf and that of well over a dozen other former U.S. Government national security officials—including two former U.S. Attorneys General and a former U.S. National Cyber Director—in litigation brought by TikTok in the United States Court of Appeals for the District of Columbia Circuit.[22] That brief, which supported the U.S. government's position defending legislation signed into law earlier this year, is attached as an appendix to this testimony. The brief argues, in relevant part, that TikTok's extensive collection on data on Americans and our allies, its close ties to the CCP and the PRC government, and the CCP's influence over TikTok's algorithm, which has previously pushed pro-Chinese and anti-American content as well as actively suppressed anti-CCP content, means that TikTok, "presents a serious and unique national security threat to the United States."[23]

And while many Americans view TikTok as a tool for kid's dance videos and short-form entertainment, the sad reality is that over the course of the last decade, this Chinese-government influenced tool has become the primary source of news for Americans under the age of 30,[24] a fact that should deeply trouble all of us. Even more concerning, given the massive amount of data that TikTok collects on its users, when combined with other data stolen by Chinese government hackers targeting the U.S. Federal Government, including the security clearance files thousands of current and former U.S. Government officials holding Top Secret-Sensitive Compartmented Information (TS/SCI) clearances, and TikTok collects on its users, when combined with other data stolen by Chinese government hackers targeting private companies holding sensitive financial, health, and travel data of millions of Americans, it is clear that TikTok's data—when fed into modern artificial intelligence algorithms—can help drive future sophisticated intelligence collection and disinformation campaigns targeting American citizens and our allies.[25] Indeed, the Office of the Director of National Intelligence (ONDI) recently indicated that "China is demonstrating a higher degree of sophistication in its influence activity, including experimenting with generative AI," and noted that "TikTok accounts run by a PRC propaganda arm reportedly targeted candidates from both political parties during the U.S. midterm election cycle in 2022."[26]

III. CHINA'S EXPLOITATION OF EMERGING TECHNOLOGIES, THEFT OF INTELLECTUAL PROPERTY, AND USE OF EXTORTIVE EFFORTS TO UNDERMINE U.S. AND ALLIED LEADERSHIP GLOBALLY

Likewise, at the core of the national security threat that the PRC poses to the United States, as well as our global competition with China for supremacy—whether in the economic, political, military, or social spheres—is technological innovation, including access to and control over critical emerging technologies, particularly in

---

[19] See, e.g., Michael Nienaber, Germany to Cut Huawei From 5G Core Network by End-2026, BNN Bloomberg (July 11, 2024), available online at <https://www.bnnbloomberg.ca/business/company-news/2024/07/10/germany-agrees-to-strip-huawei-from-5g-core-network-by-end-2026/>.

[20] See, e.g., Arjun Gargeyas, China's '2035 Standards' Quest to Dominate Global Standard-Setting, Hinrich Foundation (Feb. 21, 2023), available online at <https://www.hinrichfoundation.com/research/article/trade-and-geopolitics/china-2035-standards-project-restructure-global-economy/>

[21] See, e.g., Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118–50, div. H, 138 Stat. 955 (2024); The White House, Protecting Americans' Sensitive Data from Foreign Adversaries, 86 Fed. Reg. 31423 (June 9, 2021); The White House, Addressing the Threat Posed by TikTok, 85 Fed. Reg. 48637–38 (Aug. 6, 2020).

[22] See Brief of Former National Security Officials, TikTok Inc. and ByteDance Ltd. v. Merrick B. Garland, No. 24–1113 (consolidated with others), Document #2067987 (filed Aug. 2, 2024) (attached hereto as Exhibit A).

[23] Id. at 1–7, 11–14.

[24] Id. at 10–11.

[25] Id. at 3–10.

[26] See Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community (Feb. 5, 2024), at 12, available online at <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>.

the artificial intelligence domain.[27] In recent decades, the PRC has made aggressive moves to build its own technological innovation base and now seeks to expand those capabilities.[28] Much of this effort by the PRC initially began by actively seeking to dominate the manufacturing market for technology goods, producing equipment at costs well below those achievable in most other economies.[29] This was achieved, in significant part, by exploiting the PRC's theft of U.S. intellectual property at industrial scale—referred to as the greatest transfer of wealth in modern human history[30]—which was then leveraged to create an entire industry of state-owned and state-influenced enterprises that, when combined today, generate a tremendous amount of the technology products and capabilities sold around the globe, including producing goods on behalf of a number of highly innovative American companies, competing with others, and replacing or coopting yet others in the global market.[31] Worse still, the PRC is now going well beyond manufacturing-at-scale and is creating innovation on top of this stolen IP and securing its access to data, as it recognizes that whichever nation dominates the technology revolution—particularly in emerging technology areas like quantum computing, biotechnology, and artificial intelligence (the latter of which is particularly data reliant)—will likely also win the larger geopolitical competition.[32]

A key aspect of the PRC's effort to lead in the technology domain is its centralized planning efforts that have been in place for well over a decade, including its Made in China 2025 line of effort ("PRC 2025"), a "broad set of industrial plans that aim to boost competitiveness by advancing China's position in the global manufacturing value chain, 'leapfrogging' into emerging technologies, and reducing reliance on foreign firms."[33] This effort aims to enable China to "make major technology break-

---

[27] See, e.g., The White House, National Security Strategy (Oct. 2022), at 23, available online at <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf> ("The PRC is the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it . . . It is using its technological capacity and increasing influence over international institutions to create more permissive conditions for its own authoritarian model, and to mold global technology use and norms to privilege its interests and values."); Xi Jingping, Speech to Members of the Chinese Academy of Sciences, the Chinese Academy of Engineering, and the National Congress of China Association for Science and Technology (May 28, 2021) (translated by Zichen Wang), available online at <https://www.pekingnology.com/p/xi-jinpings-speech-on-science-and?s=r> ("[S]cientific and technological innovation has become the main battlefield of the international strategic game, and the competition around the commanding heights of science and technology is unprecedentedly fierce.").

[28] See, e.g., Tarun Chhabra, et. al, Executive Summary—Global China: Assessing China's Growing Role in the World, Brookings Institution (Apr. 2020), available online at <https://www.brookings.edu/articles/global-china-technology/> ("China's rapid technological advances are playing a leading role in contemporary geopolitical competition . . . .While the U.S. has maintained its position as the technologically dominant power for decades, China has made enormous investments and implemented policies that have contributed significantly to its economic growth, military capability, and global influence. In some areas, China has eclipsed, or is on the verge of eclipsing, the United States—particularly in the rapid deployment of certain technologies."); Bloomberg News, How China Aims to Counter US 'Containment' Efforts in Tech, Washington Post (Mar. 30, 2023), available online at <https://www.washingtonpost.com/business/2023/03/30/explainer-how-china-aims-to-counter-us-containment-efforts-in-tech/cea71f0c-cf1d-11ed-8907-156f0390d081—story.html> ("Chinese President Xi Jinping . . . and his new lieutenants are deploying what they call a "whole nation" system: marshaling resources and companies from across the country—and trillions of dollars—to drive research and development.").

[29] See Wayne M. Morrison, China's Economic Rise: History, Trends, Challenges, and Implications for the United States, Congressional Research Service (June 25, 2019), at 23, available online at <https://crsreports.congress.gov/product/pdf/RL/RL33534> ("China's abundance of low-cost labor has made it internationally competitive in many low-cost, labor-intensive manufactures. As a result, manufactured products constitute a significant share of China's trade. A substantial amount of China's imports is comprised of parts and components that are assembled into finished products, such as consumer electronic products and computers, and then exported.")

[30] See Jaffer, Addressing the National Security Threat, supra at n. 11.

[31] See, e.g., Special Competitive Studies Project, Generative AI: The Future of Innovation Power (Oct. 2023), at 3 & n.6 (collecting sources), 10–12 and 23, available online at <https://www.scsp.ai/wp-content/uploads/2023/10/economy.pdf>; Brady Helwig, et al., National Action Plan for Advanced Compute & Microelectronics, Special Competitive Studies Project (Nov. 2023), at 8–9, 13, 32, and 39, available online at <https://www.scsp.ai/wp-content/uploads/2023/11/National-Action-Plan-for-U.S.-Advantage-in-Advanced-Compute-and-Microelectronics.pdf>; see also, e.g., John Miller & Sacha Wunsch-Vincent, High-Tech Trade Rebounded Strongly in the Second Half of 2020, with New Asian Exporters Benefiting (Mar. 15, 2021), available online at <https://www.wipo.int/pressroom/en/news/2021/news__0001.html>.

[32] Id.

[33] See Karen M. Sutter, "Made in China 2025" Industrial Policies: Issues for Congress, Congressional Research Service (Mar. 10, 2023), at 1, available online at <https://crsreports.Congress.gov/product/pdf/IF/IF10964>.

throughs, lead innovation in specific industries, and set global standards" by 2035 and "[l]ead global manufacturing and innovation with a competitive position in advanced technology and industrial systems" by 2049, with key areas of focus including next generation IT and telecommunications capabilities, high performance computing, advanced robotics, and artificial intelligence.[34] And in the critically important AI domain, China released a plan back in 2017—long before the public advent of highly capable generative AI in 2022 and even well prior to the enactment of the U.S. National AI Initiative Act of 2020—to "lead the world in AI by 2030."[35] While ostensibly emphasizing domestic development in these national plans, it is clear that the PRC plans to continue to rely on the "acquisition, absorption, and adaptation of foreign technology by PRC entities that recast these capabilities as their own,"[36] and then build upon these stolen technologies to create additional innovation.

And in February of this year, the Director of National Intelligence released her Annual Threat Assessment, which she describes China's efforts to "become a world [science & technology] superpower and to use this technological superiority for economic, political, and military gain."[37] According to ODNI, "Beijing is trying to fast-track its S&T development through investments, intellectual property (IP) acquisition and theft, cyber operations, talent recruitment, scientific and academic collaboration, and illicit procurements," and noted specifically that "[i]n 2023, a key PRC state-owned enterprise has signaled its intention to channel at least $13.7 billion into emerging industries such as AI, advanced semiconductors, biotechnology, and new materials."[38]

As noted above, China's acquisition of U.S. and allied emerging technology takes place through a range of vectors: (1) outright theft of intellectual property;[39] (2) forced technology transfer from companies seeking to enter the Chinese market;[40] (3) requiring new market entrants to establish joint ventures with PRC companies;[41] (4) requiring sensitive IP to be kept in China;[42] (5) tax incentives to get production and R&D moved to China;[43] (6) acquisition of American and allied companies with sensitive technologies directly or through bankruptcy proceedings;[44] (7) corporate and government partnerships with U.S. companies, universities, and individual experts or academics, including through PRC talent programs and educational pipeline work;[45] and (8) joining and setting the agenda for international standards setting bodies.[46] And China has doubled down on these efforts, making clear that it will continue to exploit its foreign research connections, use domestic regulatory measures and influence abroad in areas like antitrust, IP, and inter-

---

[34] Id.

[35] See SCSP, Generative AI, supra at n. 31, at 3 & n. 6.

[36] Id.

[37] See ODNI, Annual Threat Assessment, supra n. 26 at 9.

[38] Id.

[39] See, e.g., Office of the U.S. Trade Representative, 2023 Special 301 Report, Executive Office of the President, The White House (Apr. 2023), at 9, 22–23, 45–47, available online at <https://ustr.gov/sites/default/files/2023-04/2023Special301Report.pdf>; see also Keith B. Alexander and Jamil N. Jaffer, China Is Waging Economic War on America. The Pandemic Is an Opportunity to Turn the Fight Around, Barron's (August 4, 2020), available online at <https://www.barrons.com/articles/china-is-waging-cyber-enabled-economic-war-on-the-u-s-how-to-fight-back-51596587400>.

[40] Id.

[41] See, e.g., Sean O'Connor, How Chinese Companies Facilitate Technology Transfer from the United States, U.S.-China Economic Security Review Commission, at 7 (May 6, 2019), available online at <https://www.uscc.gov/sites/default/files/Research/HowChineseCompaniesFacilitateTechTransferfromtheUS.pdf>

[42] Id. at 8.

[43] See, e.g., Erica York, et al., Comparing the Corporate Tax System in the U.S. & China, Tax Foundation, at 4 (May 2022), available online at <https://files.taxfoundation.org/20220502152914/Comparing-the-Corporate-Tax-Systems-in-the-United-States-and-China.pdf>.

[44] See, e.g., Cory Bennet & Bryan Bender, How China Acquires 'The Crown Jewels' of U.S. Technology, Politico (May 22, 2018), available online at <https://www.politico.com/story/2018/05/22/china-us-tech-companies-cfius-572413>; Camille A. Stewart, Full Court Press: Preventing Foreign Adversaries from Exfiltrating National Security Technologies Through Bankruptcy Proceedings, 10 J. Nat'l Security L. & Pol'y 277, 279–82 (2019).

[45] See, e.g., Alison Snyder, China Talent Program Increased Young Scientists' Productivity, Study Says, Axios (Jan. 10, 2023), available online at <https://www.axios.com/2023/01/10/china-funding-young-scientists-productivity>; see also Emily S. Weinstein, Chinese Talent Program Tracker, Center for Security and Emerging Technology, Georgetown University (Nov. 2020), available online at <https://cset.georgetown.edu/publication/chinese-talent-program-tracker/>; Federal Bureau of Investigation, The China Threat—Chinese Talent Plans Encourage Trade Secret Theft, Economic Espionage, Federal Bureau of Investigation, available online at <https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans>.

[46] See Gargeyas, China's '2035 Standards' supra n. 20.

national standards,[47] as well as make massive investments into key emerging technology areas, including quantum computing, robotics, artificial intelligence, and cybersecurity,[48] both directly and by offering low-interest and no-interest loans and massive state-driven subsidies—totaling well-over a trillion dollars—to enable its companies to compete more favorably in global markets,[49] while also using board seats to influence corporate decisionmaking.[50]

We know also that China continues to build out its STEM workforce, proactively recruiting leading STEM players from around the world,[51] and, having already passed the U.S. in the number of annual Ph.Ds awarded many years back, some estimate that the PRC may annually graduate nearly double the number of STEM Ph.Ds as the U.S. in the near future.[52] All of these efforts are also buttressed by China's longer-term efforts to secure its access to critical minerals, strategic metals, and energy resources, from production to processing,[53] and its parallel efforts to exclude U.S. and allied partners from access to such resources, all of which are critical to our technological and industrial innovation base.[54]

IV. CHINA'S EFFORT TO HOLD AMERICAN AND ALLIED CRITICAL INFRASTRUCTURE AT RISK AND INFLUENCE AMERICAN AND ALLIED VIEWS

According to ODNI, "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks."[55] ODNI noted that "PRC operations discovered by the U.S. private sector probably were intended to pre-position cyber attacks against infrastructure in Guam and to enable disrupting communications between the United States and Asia" and it assesses that "[i]f Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets . . . [in] a strike [that] would be designed to deter U.S. military action by impeding U.S. decisionmaking, inducing societal panic, and interfering with the deployment of U.S. forces."[56]

---

[47] See Sutter, Made in China 2025, supra n. 33 at 2 ("Similarly, the FYP calls for an expanded use of antitrust, IP, and standards tools—in China and extraterritorially—to set market terms and promote the export of MIC2025 goods and services now coming to market. The FYP also emphasizes the value of China's foreign research ties in developing China's own competencies in a range of MIC2025 technology areas.").

[48] See id.

[49] See, e.g., Jill C. Gallagher, U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests, Congressional Research Service (Jan. 5, 2022), at 7–8, available online at <https://crsreports.congress.gov/product/pdf/R/R47012/2> (describing how "[n]ational champions [in China], including Huawei, received preferential policy treatment, access to low-cost financing, R&D funding, and tax benefits"); see also, e.g., Ann Harrison, et al., Can a Tiger Change Its Stripes? Reform of Chinese State-Owned Enterprises in the Penumbra of the State, NBER Working Paper No. 25475 (Jan. 2019), at 24, available online at <https://www.nber.org/system/files/working_papers/w25475/w25475.pdf> (noting that former Chinese state-owned enterprises, like SOEs themselves, generally "retain ready access to large loans, concessionary interest rates, and outright subsidies").

[50] See, e.g., Scott Livingston, The New Challenge of Communist Corporate Governance, Center for Strategic & International Studies (Jan. 2021), at 2–4, available online at <https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210114_Livingston_New_Challenge.pdf>.

[51] See, e.g., Eric Schmidt, To Compete With China on Tech, America Needs to Fix Its Immigration System, Foreign Affairs (May 16, 2023), available online at <https://www.foreignaffairs.com/united-states/eric-schmidt-compete-china-tech-america-needs-fix-its-immigration-system> ("While the United States' dysfunctional system increasingly deters the world's top scientists, researchers, and entrepreneurs, other countries are proactively recruiting them. China is particularly active in doing so, with direction coming from the very top.").

[52] See, e.g., Karin Fischer, China Outpaces U.S. in STEM, Georgetown Center for Security and Emerging Technology, Latitudes (Aug. 9, 2021), available online at <https://cset.georgetown.edu/article/china-outpaces-u-s-in-stem/>. ("China could graduate nearly twice as many STEM PhDs as the United States by 2025 . . . China overtook the U.S. in PhD production in 2007 and has steadily increased its lead ever since.").

[53] See Jane Nakano, The Geopolitics of Critical Minerals Supply Chains, Center for Strategic & International Studies, at 5 (March 2021), available online at <https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210311_Nakano_Critical_Minerals.pdf>.

[54] See, e.g., Arjun Kharpal, What are Gallium and Germanium? China Curbs Exports of Metals Critical to Chips and Other Tech, CNBC (July 4, 2023), available online at <https://www.cnbc.com/2023/07/04/what-are-gallium-and-germanium-china-curbs-exports-of-metals-for-tech.html>; see also Mai Nguyen, China's Rare Earths Dominance in Focus After it Limits Germanium & Gallium Exports, Reuters (July 5, 2023), available online at <https://www.reuters.com/markets/commodities/chinas-rare-earths-dominance-focus-after-mineral-export-curbs-2023-07-05/>.

[55] See ODNI, Annual Threat Assessment, supra n. 26 at 12

[56] Id.

And just a few days earlier, the FBI Director had gone perhaps further saying, "[t]here has been far too little public focus on the fact that PRC hackers are targeting our critical infrastructure—our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems—and the risk that poses to every American . . . .China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities."[57] Providing a bit more detail on the targeting of American infrastructure, the FBI Director explained that the FBI and "our partners identified hundreds of routers that had been taken over by the PRC state-sponsored hacking group known as Volt Typhoon," which contained "malware [that] enabled China to hide, among other things, pre-operational reconnaissance and network exploitation against critical infrastructure like our communications, energy, transportation, and water sectors." According to the FBI Director, these efforts represented "[s]teps China was taking . . . to find and prepare to destroy or degrade the civilian critical infrastructure that keeps us safe and prosperous . . . represent[ing] real-world threats to our physical safety."[58]

And the Cybersecurity and Infrastructure Security Agency (CISA), in a document jointly released by CISA, FBI, NSA, and a number of other Federal and foreign intelligence agencies from Australia and New Zealand, indicated that this new posture—installing capabilities that could have a clear potential disruptive effect—said, "Typhoon's choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions."[59]

And just a few days ago, the FBI announced that it had taken down a widespread Chinese botnet, associated with a threat actor named Flax Typhoon which had infected over a quarter-million devices across North America, South America, Europe, Africa, Southeast Asia and Australia with malware.[60] This botnet, which was ostensibly focused on espionage, not disruption, nonetheless demonstrated the scale and access of Chinese hacking, with over half the devices, made up of "home routers, firewalls, storage devices, and Internet of Things devices like cameras and video recorders," being located in the U.S. And, perhaps more troublingly, the FBI noted that the Flax Typhoon actors "shared some of the infrastructure for its attacks" with the Volt Typhoon actors.[61]

Moreover, it's not just hacking or disruptive attacks that are in play; we also increasingly see the CCP actively taking a page out of the Russian covert influence playbook by seeking to, in the words of ODNI, "sow doubts about U.S. leadership, undermine democracy, and extend Beijing's influence."[62] According to ODNI, "Beijing's information operations primarily focus on promoting pro-China narratives, refuting U.S.-promoted narratives, and countering U.S. and other countries' policies that threaten Beijing's interests, including China's international image, access to markets, and technological expertise" and that it is now also seeking to "actively exploit perceived U.S. societal divisions using its online personas" and "mold U.S. public discourse—particularly on core sovereignty issues, such as Hong Kong, Taiwan, Tibet, and Xinjiang," while also potentially seeking to "influence the U.S. elections in 2024 at some level because of its desire to sideline critics of China and magnify U.S. societal divisions."[63]

All of these efforts demonstrate a commitment on the part of the CCP to get significantly more aggressive in the cyber domain, even as we recall that back in 2019, ODNI assessed that "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States" and that Russia

---

[57] See Christopher A. Wray, Director Wray's Opening Statement, House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (Jan 31, 2024), available online at <https://www.fbi.gov/news/speeches/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party>.

[58] Id.

[59] See CISA, et al., PRC State-Sponsored Actors Compromise and Maintain Persistent Access, supra n. 12.

[60] See Sam Sabin, Chinese Hacking "Typhoons" Threaten U.S. Infrastructure, Axios (Sept. 20, 2024), available online at <https://www.axios.com/2024/09/20/china-critical-infrastructure-cyberattacks>.

[61] Id.

[62] See ODNI, Annual Threat Assessment, supra n. 26 at 12.

[63] Id.

could do much of the same with respect to electrical distribution networks, while Iran could also do much the same to a large company's corporate network. [64]

V. CHINA AND RUSSIA'S EFFORTS TO USE THE INTERNATIONAL SYSTEM TO ACHIEVE THEIR GOALS

Finally, it may also be worth noting the efforts of China and Russia to use the international system, including the U.N. and various international standards setting bodies to achieve their own goals. China, for its part, has engaged in an effort to obtain additional influence in global organizations technical standard-setting bodies "by increasing the number of Chinese officials, technocrats, and private sector leaders for key leadership positions in major working groups and technical committees of international technical standard-setting bodies" [65] which it reportedly has used to "push[] for the acceptance of Chinese businesses' standards as the de facto international technical standards in several crucial sectors," and its "'Standards 2035' project also aims for the country to go global with its technical standards, especially by strategically employing its high-level officials and leaders of domestic technology enterprises at the organizations responsible for determining global technical standards." [66] And more recently, according ODNI, "China also announced [an] Global AI Governance Initiative to bolster international support for its vision of AI governance." [67]

Russia and China also recently got a significant win in the international realm with respect to a major cyber policy initiative, the U.N. Convention Against Cybercrime, with the Russian-led text—with some compromise language, to be fair—being adopted by consensus action of the Ad-Hoc Committee on Cybercrime last month. [68] For years, the United States pushed back against the Russian-proposed language and process, which it historically viewed as being overly aggressive and subject to manipulation and abuse by authoritarian regimes. [69] While the U.S. supported certain provisions of the treaty as being an appropriate exercise of law enforcement authority for nation-states, as at larger level, the U.S. did not support the treaty because it lacked the type of rule-of-law safeguards that American laws typically contain. [70] More recently, however, the U.S. backed off this position and allowed the Ad-Hoc Committee to push the Russian-led language out by consensus. [71] As the convention heads to the General Assembly for approval and, if approved, ratification by just over three dozen countries for entry into force, there has been a significant backlash from both industry and non-governmental organizations, and there is some possibility that the convention may get further delayed or halted, particularly if the United States returns to its prior position of objecting to the convention writ large. [72]

VI. POTENTIAL RESPONSES TO CONSIDER IN ADDRESSING THE THREATS POSED BY GLOBAL REPRESSORS IN THE CYBER AND EMERGING TECHNOLOGIES DOMAINS

Given all this, one might ask what ought be done to address these very real challenges. Below are a few initial thoughts.

1. *Provide Appropriations for Basic Science Research and Workforce Development.* The U.S. Government has long been one of the key seed funders of critical basic science research in American universities and industry, and this has led to major breakthroughs in areas where countries like China now seek to compete including in biotechnology, high-performance computing, quantum computing, and artificial intelligence. [73] Ensuring that some of the key provisions in the CHIPS and Science

---

[64] See ODNI, Worldwide Threat Assessment of the U.S. Intelligence Community (Jan. 29, 2019), available online at <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR__SSCI.pdf>.

[65] See Gargeyas, China's '2035 Standards' Quest, supra n. 20.

[66] Id.

[67] See ODNI, Annual Threat Assessment, supra n. 26 at 9.

[68] See Agence France Presse, U.N. Approves its First Treaty Targeting Cybercrime, Barron's (Aug. 8. 2024), available online at <https://www.barrons.com/news/un-approves-its-first-treaty-targeting-cybercrime-93801d31>.

[69] See Jason Pielemeier, Rethinking the United Nations Cybercrime Treaty, Just Security (Sept. 23, 2024), available online at <https://www.justsecurity.org/100333/rethinking-united-nations-cybercrime-treaty/>.

[70] See AFP, U.N. Approves First Treaty, supra n. 68.

[71] See Pielemeier, Rethinking the U.N. Cybercrime Treaty, supra n. 69.

[72] Id.

[73] See James Manyika et al., Innovation and National Security—Keeping Our Edge, Council on Foreign Relations (Sep. 2019), at 2, 19, available online at <https://www.cfr.org/report/keeping-our-edge/pdf/TFR__Innovation__Strategy.pdf> ("federally supported R&D had a dramatic impact on U.S. competitiveness and national security. According to a 2019 study, starting in the

Act and other such legislation, including funding for next generation communications technologies and artificial intelligence, continues to be provided is critical.[74]

2. *Avoid Taking Action that Would Limit Private Sector R&D Spending and Instead Incentivize It in Critical Areas.* Today, the private sector represents 70 percent of all R&D expenditures in the United States, with technology companies leading the way, making up seven of the top ten R&D spenders, including all of the top five.[75] Core R&D spending, along with our permissive economic and legal environment and the availability of significant amounts of venture and growth capital, as well as a highly skilled workforce, is what makes America the technology innovation hub of the globe. These capabilities are not only at the heart of our economic success, they are also a core reason why our national defense capabilities remain relatively unmatched across the globe today. If we are to compete effectively with the PRC, we need to incentivize, not limit the capabilities of the top R&D investors in the U.S., including the technology companies that are in the top five R&D spenders in the Nation. To do so, we must avoid the temptation to artificially restrain successful innovators in the absence of actual, demonstrable bad behavior, while also providing new tax and other economic incentives for increased private R&D investment—both for new entrants as well as existing players that can scale—in a range of areas like high-performance computing, quantum technology, AI/ML, trust, safety, and security, and the design and production, in the United States and allied nations, of leading-edge semiconductor capabilities.

3. *Incentivize Technology Infrastructure Investment.* For the better part of the last six decades, the United States has benefited significantly from being the core hub of the global telecommunications infrastructure. As the place where much of the world's telecommunications systems come together, particularly when it comes to global Internet traffic, the United States has been able to innovate rapidly and gain both economic and national security benefits from this convergence.[76] It is critical that the government provide the right incentivizes for industry to build out both domestic and allied computing and communications infrastructure and invest in the

---

2010's nearly one-third of patented U.S. inventions relied on federally funded science []. Touch screens, the Global Positioning System (GPS), and internet technologies central to the smartphone are all products of Defense Department research . . . Between 1988 and 2010, $3.8 billion of Federal investment in genomic research generated an economic impact of $796 billion and created 310,000 jobs. A new wave of support for basic research could have similar economic and military benefits."); see also Jamie Gaida et al., ASPI's Critical Technology Tracker: The Global Race for Future Power, Australian Strategic Policy Institute (Feb. 2023), at 1, available online at <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-03/ASPIs%20Critical%20Technology%20Tracker__0.pdf> (noting that "China's global lead extends to 37 out of 44 technologies that ASPI is now tracking, covering a range of crucial technology fields spanning defence, space, robotics, energy, the environment, biotechnology, artificial intelligence (AI), advanced materials and key quantum technology areas").

[74] See, e.g., Pub. L. No. 117–167, §§ 10101–114 (basic science); §§ 10221–235 (basic science); §§ 10311–321 (STEM education & workforce) & §§ 10501–526 (STEM education & workforce); see also Madeline Ngo, CHIPS Act Funding for Science and Research Falls Short, New York Times (May 30, 2023), available online at <https://www.nytimes.com/2023/05/30/us/politics/chips-act-science-funding.html> ("The total funding for research agencies was nearly $3 billion short of authorized levels this year, according to a recent Brookings Institution analysis . . . [T]he director of the National Science Foundation[] said the money would help the Nation lead in industries that were listed as key focus areas in the law, such as artificial intelligence and biotechnology … [and] could also help the agency expand A.I. research and training programs aimed at building up the nation's STEM work force, which agency officials said were critical since the country is facing a shortage of workers to build semiconductors."); see also Matt Hourihan, Analysis: As Congress Considers COMPETES, How Short Are We From The Old COMPETES?, American Association for the Advancement of Science (Feb. 22, 2022), available online at <https://www.aaas.org/sites/default/files/2022-02/AAAS%20COMPETES%20Shortfalls%20Feb%20__2022__0.pdf>.

[75] See Jamil N. Jaffer, NSI Backgrounder: The Role of American Technology Sector in Safeguarding U.S. Economic and National Security, National Security Institute, GMU Scalia Law School (Dec. 2022), at 1 & n. 6, available online at <https://nationalsecurity.gmu.edu/the-role-of-american-technology-sector-in-safeguarding-u-s-economic-and-national-security/> (citing John F. Sargent, U.S. Research and Development Funding and Performance: Fact Sheet, Congressional Research Service (Sept. 13, 2022), available online at <https://crsreports.congress.gov/product/pdf/R/R44307/18>); see id. at 1 & n. 5 (citing Prableen Bajpai, Which Companies Spend the Most in Research and Development (R&D)?, Nasdaq (June 21, 2021), available online at <https://www.nasdaq.com/articles/which-compa-nies-spend-the-most-in-research-and-development-rd-2021-06-21>).

[76] Cf. Manyika et al., Innovation and National Security, supra n. 73 at 2, 19, available online at<https://www.cfr.org/report/keeping-our-edge/pdf/TFR__Innovation__Strategy.pdf> ("This seventy-year strength arose from the expansion of economic opportunities at home through substantial investments in education and infrastructure, unmatched innovation and talent ecosystems, and the opportunities and competition created by the opening of new markets and the global expansion of trade. ").

capacity and innovation to deliver such capabilities globally while also continuing efforts to rip and replace adversary gear, whether it is in state, local or allied systems. To that end, the government should provide tax and other economic incentives for increased private investment in the development of such technologies, the broader deployment of large-scale computing infrastructure to support cloud and edge computing, the replacement of adversary technology, and the expansion of AI capabilities being made available to U.S. and allied innovators.

4. *Maintain U.S. Capacity for Innovation.* Ensuring that the United States is able to access the underlying manufacturing capacity and workforce necessary to support a modern technology and communications infrastructure—including consistent access to semiconductors, critical minerals, and other core materials necessary to support major technological innovation—will also be of strategic importance to the United States in the coming years. It is critical that government and industry work together to create the right tax and regulatory incentives to ensure that American and allied companies invest their money here (and in allied nations) to create much-needed capacity and to ensure that we have the skilled workers necessary to build and maintain this capacity.

5. *Avoid Harmful Overregulation.* To ensure that the United States remains a leader in technology innovation, it is critical that the United States avoid adopting significant new regulatory or administrative policies that would undermine the ability of the United States to effectively compete on a global scale. Efforts in recent years to amend longstanding and highly effective antitrust laws that have served our economy well for decades,[77] are a key example of the kind of new policies that would be highly detrimental in the context of the ongoing economic and national security competition with China. These efforts, which target a handful of technology companies based on the nature and scale of their business, are largely driven by policy issues unrelated to innovation or competition.[78] As such, they would likely undermine the very companies that have the largest potential to benefit the United States and our allies by posing the biggest threat to the PRC's effort to win the technology competition and sends exactly the wrong message to new entrants: namely, that if small, innovative businesses thrive and become highly successful, expanding not through unfair competition, but through market success, the government might seek to target them for special attention, creating laws to cut them down to size.[79] To the extent there are concerns that market power actually is being used to undermine competition, existing law—and the longstanding consumer welfare standard that undergirds them—when used appropriately, can effectively address these concerns.[80]

6. *Avoid Being Tempted By the European Model.* There are those who argue that the U.S. ought enact laws like the General Data Protection Regulations, the Digital Markets Act, the Digital Services Act, and the AI Act in order to make sure we are

---

[77] See, e.g., American Innovation and Choice Online Act, S. 2992, 117th Cong. (2021); Open App Markets Act, S. 2710, 117th Cong. (2021).

[78] Bill Evanina & Jamil N. Jaffer, Kneecapping U.S. Tech Companies Is a Recipe for Economic Disaster, Barron's (June 17, 2022), available online at <https://www.barrons.com/articles/kneecapping-u-s-tech-firms-is-a-recipe-for-economic-disaster-51655480902> ("Conservatives are often worried—sometimes for good reason—that certain social or mainstream media companies might actively seek to suppress or quiet conservative voices. On the liberal side, there are a range of legitimate concerns with technology companies, including the displacement of traditional labor in the new gig economy . . . Yet rather than tackling these concerns directly by going after the specific behaviors or actions that trouble ordinary Americans, politicians in Washington have chosen instead to vilify some of our most successful companies and to go after them economically."); see also David R. Henderson, A Populist Attack On Big Tech, The Hoover Institution (Mar. 3, 2022), available online at <https://www.hoover.org/research/populist-attack-big-tech-0>.

[79] Klon Kitchen & Jamil Jaffer, The American Innovation & Choice Online Act Is A Mistake, The Kitchen Sync (Jan. 19, 2022), available online at <https://www.thekitchensync.tech/p/the-american-innovation-and-choice> ("Going after our technology companies, particularly a targeted shot at certain big ones, sends the wrong message to startups and investors alike; it tells them that if you are innovative enough to be successful and grow significantly larger, you may be targeted for different treatment … This undermines not only the companies that are likely to be investing in R&D over the next decade and generating some of the key innovations that will contribute to our national security, it also undermines a central proposition that has created a robust tech ecosystem in this country: take risk, innovate, fail fast and often, and when you succeed, reap the rewards so long as you don't exploit your position to gain unfair advantage."); Evanina & Jaffer, Kneecapping U.S. Tech Companies, supra n. 78 ("Picking and choosing individual companies to be treated differently than others under our antitrust laws is inconsistent with the heart of our economic system, which Seeks to reward innovation and success, not penalize them.").

[80] See Henderson, A Populist Attack on Big Tech, supra n. 78; Evanina & Jaffer, Kneecapping U.S. Tech Companies, supra n. 78.

keeping up on the latest in regulatory creep.[81] The reality, however, if one looks at the economic and innovation scoreboard as between the United States and Europe—when looking at GDP growth, the creation of highly successful, highly innovative businesses, or building private companies whose technology innovations have a massive benefit for national and economic security—it tilts decisively in favor of the U.S. today, as it has for the last five decades at least.[82] Unlike Europe, which often seeks to drive specific market outcomes, the United States has generally sought to institute a broadly applicable set of rules designed to ensure that all market participants compete fairly. Sticking with the traditional American approach is the right way to go.

7. *Incentivize AI and Emerging Technology Innovation and Focusing Any Regulation Only on Critical Gaps.* The approach that best protects U.S. national and economic security in AI and emerging technology is one that allows innovation to flourish, stepping cautiously to address legitimate concerns where regulation is warranted and appropriate, based on traditional considerations like a demonstrable market failure. Rather than rushing to broad-based regulation, as the European Parliament has recently, the wiser approach, consistent with the American approach to innovation, would be to identify potential regulatory need, assesses whether regulation is necessary and appropriate, and prioritize the voluntary adoption of industry-driven frameworks, before moving to a regulatory posture, which in turn would build upon the voluntary frameworks.[83] While much has been written about the potential of AI to cause significant harm, the fact is that AI has the potential to have a transformative effect on human society, raising all boats and allowing a broad range of workers to do mundane tasks more efficiently while freeing innovators to create even more productive tools and capabilities.[84] As such, the best approach on AI may be the more cautious one: encouraging those closest to the actual creation of the technology to craft potential frameworks and industry best practices that might guide the trusted, safe, and secure development and implementation of these technologies.

8. *Stop Investing in Our Adversaries.* In 2022, the total U.S. foreign direct investment in China was $126.1 billion, an increase of more than $10 billion from the prior year.[85] American companies have made major investments in leading-edge Chinese companies, including in the artificial intelligence arena, and by one metric, U.S. investors "accounted for nearly a fifth of investment deals in Chinese AI/ML companies from 2015 to 2021."[86] We must take sustainable action to limit on out-

---

[81] See, e.g., Cecilia Kang, As Europe Approves New Tech Laws, the U.S. Falls Further Behind, New York Times (April 22, 2022), available online at <https://www.nytimes.com/2022/04/22/technology/tech-regulation-europe-us.html>

[82] See Jan Rybnicek, Innovation in the United States and Europe, in Report on the Digital Economy, Global Antitrust Institute (2020), available online at <https://gaidigitalreport.com/2020/08/25/innovation-in-the-united-states-and-europe/>; Michael Ringel et al., The Most Innovative Companies 2020, The Serial Innovation Imperative, Boston Consulting Group, at 16 (June 2020), available online at <https://web-assets.bcg.com/img-src/BCG-Most-Innovative-Companies-2020-Jun-2020-R4__tcm9-251007.pdf>; see also Loren Thompson, Why Reining In Big Tech Could Be Bad News For U.S. National Security, Forbes (July 7, 2022), available online at <https://www.forbes.com/sites/lorenthompson/2022/07/07/why-breaking-up-big-tech-could-be-bad-news-for-us-national-security/?sh=1e40190d32bd>; Jaffer, The Role of American Technology Sector, supra n. 75.

[83] Cf. Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards & Technology (Apr. 16, 2018), available online at <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

[84] Compare Geoffrey Hinton, et al., Statement on AI Risk: AI Experts and Public Figures Express their Concern About AI Risk, Center for AI Risk (May 30, 2023), available online at <https://www.safe.ai/statement-on-ai-risk#open-letter> ("Mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war.") with Michael Chui, et al., Generative AI is Here: How Tools Like ChatGPT Could Change Your Business, McKinsey & Co. (Dec. 20, 2022), available online at <https://www.mckinsey.com/capabilities/quantumblack/our-insights/generative-ai-is-here-how-tools-like-chatgpt-could-change-your-business>; Danny Hajek, et al., What Is AI and How Will It Change Our Lives?, NPR (May 25, 2023), available online at <https://www.npr.org/2023/05/25/1177700852/ai-future-dangers-benefits>.

[85] See Bureau of Economic Analysis, Direct Investment by Country and Industry, 2022, U.S. Dept. of Commerce (July 20, 2023), available online at <https://www.bea.gov/sites/default/files/2023-07/dici0723.pdf>.

[86] See Emily S. Weinstein & Ngor Luong, U.S. Outbound Investment into Chinese AI Companies, Georgetown University Center for Security & Emerging Technology (Feb. 2023), at 11–13, available online at <https://cset.georgetown.edu/wp-content/uploads/CSET-U.S.-Outbound-Investment-into-Chinese-AI-Companies.pdf> see also Alexandra Alper, U.S. Investors Have Plowed Billions into China's AI sector, Report Shows, Reuters (Feb. 1, 2023), available online at

Continued

bound investment from the U.S. in critical industries like high performance computing, semiconductors, critical minerals, cloud computing, artificial intelligence, and quantum computing, to name just a few.

9. *Growing a STEM-Capable Workforce By Investing Here and Fixing Our Broken Immigration System.* The U.S. must take action to grow our STEM workforce, including continuing appropriate funding the workforce-related programs authorized in the CHIPS and Science Act and directing new and existing resources to the States in form of block grants to be used through public schools, public charter schools, and private institutions.[87] We must also incentivize those who come from abroad to study here to stay here, develop their new technology, and build businesses in the United States, rather than forcing them to back home. One of the nation's most enduring achievements is our "ability to attract and retain some of the world's best STEM talent . . . [that can] drive research and development efforts," yet our current immigration system makes little sense, because it allows a wide range of undergraduate and graduate students to benefit from our world-class higher education system, but then—with exception of the small number that are able to obtain H–1B visas or otherwise stay in the United States—requires them to return home to build businesses abroad.[88] This poorly thought-out policy actually forces American companies to hire high-skilled workers abroad and deprives our own economy of the benefits of their employment here, including the tax revenues and spending of these high-skilled, high-wage workers who could easily be vetted to address any potential IP theft and foreign intelligence concerns.[89]

10. *Set a Clear, Declaratory Cyber Deterrence Policy and Where Needed Take Action to Deter Future Attacks.* If we are to take seriously the threat posed by China and other nations that are actively targeting our critical infrastructure, we cannot simply remain on the defensive; rather, we must implement effective deterrence in the cyber domain. We can do so being clear about what kind of activity we can tolerate and what kind of activity would cross a line; we must talk about our offensive capabilities in the cyber domain to demonstrate one way we might effectuate that deterrence; and, having established a clear line, we must be willing to enforce it and impose significant consequences on bad actors and we must do so in a way that is open and transparent so we are able to deter both the current and future actors.[90] While there are those that argue such a policy is too provocative or more likely to get us into a conflict, the reality is that we are already in state of sustained low-level combat in the cyber domain, and that it has gotten worse in recent years not better.[91] The fact of the matter is that when our adversaries don't know how we might react—or worse, based on prior practices assume that we won't react all—they are more likely to push the envelope and test our boundaries.[92]

<https://www.reuters.com/technology/us-investors-have-plowed-billions-into-chinas-ai-sector-report-shows-2023-02-01/>.

[87] See McKinsey & Co., The CHIPS and Science Act: Here's What's in It (Oct. 4, 2022), available online at <https://www.mckinsey.com/industries/public-sector/our-insights/the-chips-and-science-act-heres-whats-in-it>; cf. National Science Teachers Association, FACT SHEET: Title IV, Part A of ESSA: Student Support and Academic Enrichment Grants and Science/STEM Education, available online at <https://static.nsta.org/pdfs/ESSATitleIV-ScienceSTEMFactSheet.pdf> (describing the $1.65 billion Student Support and Academic Enrichment block grant program under The Every Student Succeeds Act (ESSA) enacted in 2014, which consolidated the Math and Science Partnership Grants, which is described as "the largest single program at the Department of Education devoted exclusively to science/STEM-related classroom purposes," having "received $152.7M in fiscal year 2016 before it was eliminated").

[88] See William Alan Reinsch & Thibault Denamiel, Immigration Policy's Role in Bolstering the U.S. Technology Edge, Center for Strategic & International Studs. (Feb. 6, 2023), available online at <https://www.csis.org/analysis/immigration-policys-role-bolstering-us-technology-edge>; see also Gina M. Raimondo, Remarks by U.S. Sec'y of Com. Gina Raimondo on the U.S. Competitiveness and the China Challenge, U.S. Department of Commerce (Nov. 20, 2022), available online at https://www.commerce.gov/news/speeches/2022/11/remarks-us-secretary-commerce-gina-raimondo-us-competitiveness-and-china>; see also Eric Schmidt, To Compete With China on Tech, America Needs to Fix Its Immigration System, Foreign Affairs (May 16, 2023), available online at <https://www.foreignaffairs.com/united-states/eric-schmidt-compete-china-tech-america-needs-fix-its-immigration-system>.

[89] See Paayal Zaveri, America's Immigration System is a Nightmare & it's Forcing Tech Companies to Move Jobs Outside of the Country, Business Insider (Mar. 14, 2023), available online at <https://www.businessinsider.com/us-tech-firms-offshoring-immigration-labor-shortage-issues-remote-work-2023-3>.

[90] See Jamil N. Jaffer, Statement for the Record, Safeguarding the Federal Software Supply Chain, Subcommittee on Cybersecurity, Information Technology, and Government Innovation, Committee on Oversight and Accountability (Nov. 29, 2023), available online at <https://oversight.house.gov/wp-content/uploads/2023/11/Written-Statement-Jaffer.pdf>.

[91] Id.

[92] Id.

VII. CONCLUSION

For over a decade now, Congress and the executive branch have been talking the very real threats that globally repressive nations like China, Russia, Iran, and North Korea pose to the United States, particularly in the cyber domain and with respect to emerging technologies. And while we have taken significant action to address some of these threats, the reality is that we are far from where we need to be if we are going to successfully limit the threat these nations pose. It is critical that the United States take swift action, alongside our allies, to limit the threats we face in the cyber domain and to limit our exposure to the threats that are apparent in the emerging technology domain as well while continuing to lead on innovation. To do any less would be significant mistake.

EXHIBIT A

ORAL ARGUMENT SCHEDULED FOR SEPTEMBER 16, 2024

No. 24-1113, 24-1130, 24-1183

UNITED STATES COURT OF APPEALS
FOR THE D.C. CIRCUIT

TIKTOK INC. AND BYTEDANCE LTD.,

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

consolidated with

caption continued on inside cover

On Petitions for Review of Constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act

BRIEF OF AMICI CURIAE FORMER NATIONAL SECURITY OFFICIALS

Thomas R. McCarthy
Kathleen S. Lane
CONSOVOY MCCARTHY PLLC
1600 Wilson Blvd., Ste. 700
Arlington, VA 22209
(703) 243-9423
tom@consovoymccarthy.com
katie@consovoymccarthy.com

August 2, 2024

Counsel for Amici Curiae

BRIAN FIREBAUGH, CHLOE JOY SEXTON, TALIA CADET, TIMOTHY MARTIN, KIERA SPANN, PAUL TRAN, CHRISTOPHER TOWNSEND, and STEVEN KING

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

BASED POLITICS INC.

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rules 26.1 and 28(a)(1) and Fed. R. App. 26.1 the undersigned counsel certifies as follows:

A. Parties and Amici

The parties to *TikTok Inc. v. Garland*, No. 24-1113, are Petitioners TikTok Inc and ByteDance Ltd., and Respondent Merrick B. Garland, in his official capacity as Attorney General of the United States. The parties to the first consolidated case, *Firebaugh v. Garland*, No. 24-1130, are the Creator Petitioners and Respondent Garland, in his official capacity as Attorney General of the United States. The parties to the second consolidated case, *BASED Politics Inc. v. Garland*, No. 24-1183, are Petitioner BASED Politics Inc. and Respondent Garland, in his official capacity as Attorney General of the United States. As of the finalization of this brief, the following amici have either filed a brief or a notice of intent to participate: Electronic Frontier Foundation, Freedom of the Press Foundation, TechFreedom, Media Law Resource Center, Center for Democracy and Technology, First Amendment Coalition, Freedom to Read Foundation, The Cato Institute, Professor Matthew Steilen, Arizona Asian American Native Hawaiian and Pacific Islander for Equity Coalition, Asian

American Federation, Asian Americans Advancing Justice Southern California, Calos Coalition, Hispanic Heritage Foundation, Muslim Public Affairs Council, Native Realities, OCA-Asian Pacific American Advocates of Greater Seattle, South Asian Legal Defense Fund; Sikh Coalition, Sadhana, San Francisco, Knight First Amendment Institute at Columbia University, Free Press, Pen American Center, Milton Mueller, Timothy H. Edgar, Susan A. Aaronson, Hans Klein, Hungry Panda US, Inc., Shubhangi Agarwalla, Enrique Armijo, Derek Bambauer, Jane Bambauer, Elettra Bietti, Ashutoh Bhagwat, Stuart N. Brotman, Anupam Chander, Erwin Chemerinsky, James Grimmelmann, Nikolas Guggenberger, G.S. Hans, Robert A. Heverly, Michael Karanicolas, Kate Klonick, Mark Lemley, David S. Levine, Yvette Joy Liebesman, Dylan K. Moses, Sean O'Brien, Christopher J. Sprigman.

Because these petitions were filed directly in this Court, there were no district court proceedings in any of the cases.

B. Rulings Under Review

The petitions seek direct review of the constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act

(H.R. 815, Div. H, 118th Cong., Pub. L. No. 118-50 (April 24, 2024). There were no district court proceedings in any of the cases.

C. Related Cases

Amici are not aware of any other case pending before this or any other court that is related.

Dated: August 2, 2024

/s/ Thomas R. McCarthy
Thomas R. McCarthy

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Regulations

Executive Branch Sources

Congressional Sources

News Sources

Other Authorities

GLOSSARY

Act	Protecting Americans from Foreign Adversary Controlled Applications Act
CCP	Chinese Communist Party
DNI	Director of National Intelligence
FBI	Federal Bureau of Investigation
OMB	Office of Management and Budget
OPM	Office of Personnel Management

INTEREST OF AMICI CURIAE

Amici curiae are former national security government officials in their individual capacities.[1] Amici are filing this brief to address the national security concerns surrounding TikTok, ByteDance, and those entities' ties to a foreign adversary—the Chinese Communist Party.

Amici have served at the highest levels of government, in national security, intelligence, and foreign policy roles. They have served under different administrations, for leaders of different political parties, during different global conflicts, and have different foreign policy concerns. Despite their differences, amici have all served with a common goal and purpose: securing this Nation and protecting it from foreign threats. TikTok presents one such critical foreign threat. As former government officials and as national security experts, amici have a strong interest in ensuring that the Court understands and appreciates the national security interests at stake in this litigation. Amici are identified in Appendix A.

[1] No counsel for a party authored this brief in whole or in part, and no party or counsel for a party made a monetary contribution intended to fund its preparation or submission. No person other than the amici or their counsel made a monetary contribution to the preparation or submission of this brief.

SUMMARY OF ARGUMENT

Approximately 170 million Americans use TikTok. Like other social media applications, TikTok collects massive amounts of personal data on its users, and TikTok has a proprietary algorithm that curates what each user sees on the app. Unlike other social media applications, however, TikTok is subject to the direction and control of the Chinese Communist Party. Congress, recognizing the national security threat posed by CCP control over TikTok sought to address this threat by enacting the Protecting Americans from Foreign Adversary Controlled Applications Act.

TikTok is owned by a Chinese company beholden to the Chinese Communist Party. Chinese government control over TikTok affords the CCP direct access to the massive amounts of personal data of those 170 million American TikTok users, and it allows the CCP to manipulate what those Americans see and share on TikTok. The former enables the CCP to collect, use, and exploit those vast swaths of personal information for its own benefit. As FBI Director Wray put it, TikTok is "one of the most valuable surveillance tools on the planet." *Hearing on the 2023 Annual Threat Assessment of the U.S. Intelligence Community* at 1:09:00, U.S. Senate Select Comm. Intelligence Hearing (Mar. 8, 2023) (testimony

of Director Wray) ("*2023 Threat Assessment Hearing*"), https://perma.cc/3YJG-XQDJ. And the latter enables the CCP to deploy TikTok as a widescale propaganda and misinformation machine to influence American policy debates. Indeed, TikTok sent its 170 million American users a prompt mischaracterizing the Act's divestment requirement as a flat ban on TikTok and encouraging them to call their representatives in Congress to oppose the Act. Sapna Maheshwari & David McCabe, *TikTok Prompts Users to call Congress to Fight Possible Ban*, N.Y. Times (Mar. 7, 2024), https://perma.cc/GD3J-QNPV.

Amici agree with the United States that the Act is a lawful exercise of Congressional authority to protect national security and that it does not run afoul of the First Amendment or any other Constitutional proscription. Amici write separately to underscore the grave national-security threats posed by Chinese control of TikTok; to highlight TikTok's failure to take any meaningful action to reduce those threats; and to explain that the compelling national security interests behind the Act overcome any applicable level of First Amendment scrutiny.

ARGUMENT

I. The Chinese government's control of TikTok presents a novel and serious national security threat.

TikTok presents a serious and unique national security threat to the United States because the data it collects is made available to the Chinese Communist Party and its ability to influence information shared through the application is subject to the direction and control of the CCP. TikTok collects massive amounts of information about the 170 million Americans using its application. USA.Br. 1, 18-39; *House lawmakers deeply concerned over TikTok despite CEO's testimony*, CBS News (Mar. 23, 2023), https://perma.cc/H95J-PETG. TikTok acknowledges that it automatically collects, among other things, its users profile information and image; connections between individual users; content shared between users; private messages; information found in a device's clipboard; and purchase and payment information. *Privacy Policy*, TikTok (last updated July 1, 2024), https://perma.cc/RV8S-U38H. Along with this information, TikTok collects voice and location data, and, perhaps most troublingly, the application may listent to users even when they are not using the application and even when their privacy settings are set to prohibit such collection. *The Select: 'TikTok Special'-A weekly Committee Recap* (Mar.

8, 2024), https://perma.cc/Z7YH-SW9S. In the aggregate, this vast dataset provides significant and deep insights into those using TikTok's application.

What makes TikTok unique from other social-media applications is that the CCP has direct access to this vast dataset. TikTok is owned by ByteDance, a Chinese corporation that is "beholden to the CCP." *Hearing on 2024 Annual Threat Assessment* at 1:09:50, U.S. Senate Select Committee Intelligence Hearing (Mar. 11, 2024) (statement of Director Wray), https://perma.cc/5ZMS-ZVR4; *see also Annual Threat Assessment of the U.S. Intelligence Community*, DNI Office (Feb. 5, 2024), https://perma.cc/NLG3-Z6R7. And China's National Intelligence Law requires ByteDance and TikTok to assist with intelligence gathering. *Letter from Rep. Mike Gallagher to Christopher Wray, FBI Director*, at 1 (Dec. 7, 2023), https://perma.cc/R352-UFKG. This means that ByteDance must provide China's intelligence agencies with direct access to the extensive personal data TikTok collects on its more than 170 million American users. *See Safeguarding Our Future*, The National Counterintelligence and Security Center, https://perma.cc/549G-W4X2; *see also* USA.Br. 17.

Beyond the access the CCP has to the data of American citizens, it is well-documented that the CCP also has significant *internal* influence over TikTok. The CCP requires certain companies, like TikTok, to host an internal party committee, which has the "sole function" of ensuring "compliance with [CCP] orthodoxy." *See Hearing on Oversight of the Federal Bureau of Investigation* at 3:19:00, House Judiciary Committee (July 12, 2023) (statement of Director Wray), https://perma.cc/87HV-YR8D; *see also* Kevin Breuninger & Eamon Javers, *Communist Party cells influencing U.S. companies' China operations*, CNBC (July 12, 2023), https://perma.cc/TU6B-GHYV. In some cases, the company's charter directly incorporates these internal party committees, giving the CCP even more power over "management decisions" and ensuring that CCP personnel "serve in management or board positions." Scott Livingston, *The New Challenge of Communist Corporate Governance*, Ctr. for Strategic & Int'l Studies (Jan. 2021), https://perma.cc/X3KY-AYLC; *see also* Lauren Yu-Hsin Lin & Curtis J. Milhaupt, *CCP Influence over China's Corporate Governance*, Stanford Ctr. on China's Economy and Institutions (updated Nov. 1, 2022), https://perma.cc/PYL3-DDN2.

Taken together, this means that TikTok automatically collects substantial amounts of data on over 170 million Americans, which is then directly accessible by the CCP—whether through Chinese intelligence laws or through internal pressure and control from those planted within the company to carry out CCP's policy objectives. Indeed, a former TikTok executive confirmed that CCP members were specifically stationed at ByteDance in order to review data collected through TikTok, and to influence internal decisions about how the TikTok algorithm works to convey information to its users, including more than 170 million Americans. *See* Zen Soo, *Former ByteDance executive says Chinese Communist Party tracked Hong Kong protesters via data*, AP News (June 7, 2023), https://perma.cc/K9HB-XDBL; Thomas Fuller & Sapna Maheshwari, *Ex-ByteDance Executive Accuses Company of 'Lawlessness,'* N.Y. Times (May 12, 2023), perma.cc/DE96-KD7G. The pressure the CCP exerts on TikTok and its parent, ByteDance, is also readily apparent. For example, last year, ByteDance executives publicly apologized for deviating from "socialist core values" for "vulgar" content on one of its other applications. *See* Yaqiu Wang, *The Problem with TikTok's Claim of Independence from Beijing*, The Hill (Mar. 24, 2023), https://perma.cc/L44R-U9HL. And

ByteDance has used its data collection to track political activity, including activities of Hong Kong protestors and commentary by American journalists. *See* Emily Baker-White, *EXCLUSIVE: TikTok Spied on Forbes Journalists*, Forbes (Dec. 22, 2022), https://perma.cc/XUS8-ATNP; Soo, *supra*; *TikTok: How Congress Can Safeguard American Data Privacy*, Hearing Before the H. Comm. on Energy & Commerce, 118th Cong. (2023) ("*2023 House Data Privacy Hearing*"). The CCP's control over TikTok and its direct access to the personal data of 170 million Americans standing alone therefore presents grave national security concerns.

These concerns are only heightened by the fact that the Chinese government has access to massive amounts of additional highly sensitive data—data belonging to hundreds of millions of Americans that China has obtained through cyber operations undertaken by sophisticated Chinese-government intelligence and military hackers. *See, e.g.*, *Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions*, Dep't of Justice (May 9, 2019) ("*Anthem Breach*"), https://perma.cc/77P4-T7Y5; *Chinese Military Hackers Charged in Equifax Breach*, Federal Bureau of Investigation (Feb. 10, 2020) ("*Equifax Breach*"), https://perma.cc/7JPH-G2EC; David E. Sanger, et al.,

Marriott Data Breach is Traced to Chinese Hackers, N.Y. Times (Dec. 11, 2018), https://perma.cc/3EJT-BPL9; *Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, Dep't of Justice (Feb. 10, 2020), https://perma.cc/9GRX-QR4V. In the OPM breach, hackers working on behalf of the Chinese government exfiltrated over 20 million personnel records of American government employees holding Top Secret/Sensitive Compartmented Information (TS/SCI) clearances, collecting social security numbers, dates and places of birth, addresses, and detailed background check data—including "financial data; information about spouses, children and past romantic relationships; and any meetings with foreigners"—on the very government employees that the U.S. government entrusts with its most sensitive classified intelligence information. *See* Sanger, *supra*. Through the Anthem hack, the Chinese government also obtained the addresses, birth dates, and social security numbers of more than 78 million Americans and may also have obtained protected health information. *See Anthem Breach*, *supra*. Likewise, in the Equifax data breach, Chinese military hackers working for the People's Liberation Army (PLA) obtained the highly sensitive personal data of 145 million Americans—nearly half the

U.S. population—potentially including financially sensitive creditworthiness information. *See, e.g., Equifax Breach*, *supra*; *see also* Criminal Indictment, *United States v. Zhiyong*, 1:20-cr-00046, Doc. 1 (N.D. Ga. Jan. 28, 2020). And in the Marriott hack, Chinese hackers working for the Ministry of State Security, a key CCP intelligence agency, obtained the personal details of approximately 500 million guests at the "top hotel provider for American government and military personnel," including hotel stays and passport information. *See* Sanger, *supra*.

Collectively, the Chinese government has access to information about Americans' day-to-day routines from TikTok—cataloguing who these Americans interact with, what they do, and where they go—as well as access to many of these individuals' most sensitive personal information. *See US House passes bill that would ban TikTok*, Live Now Fox (Mar. 13, 2024) (statement of Jamil Jaffer), https://perma.cc/9M77-TQNW. The CCP can exploit this massive trove of sensitive data to power sophisticated artificial intelligence (AI) capabilities that can then be used to identify Americans for intelligence collection, to conduct advanced electronic and human intelligence operations, and may even be weaponized to undermine the political and economic stability of the United States

and our allies. *Id.; see also* Sanger, *supra* ("Such information is exactly what the Chinese use to … build a rich repository of Americans' personal data for future targeting."). Indeed, according to former CIA Director Gen. (Ret.) Michael Hayden, speaking about the OPM data breach specifically, there isn't "recovery from what was lost… [i]t remains a treasure trove of information that is available to the Chinese until the people represented by the information age off[]… [t]here's no fixing it." Dan Verton, *Impact of OPM breach could last more than 40 years*, FEDSCOOP (July 10, 2015), https://perma.cc/E6QH-JHLU. The combined national security impact of these hacks—when added to the sensitive social networking, location, and behavioral information on 170 million Americans available to the Chinese government through its direct access to TikTok data—is thus nearly impossible to overstate.

And it only gets worse. The CCP also uses TikTok as both a propaganda and misinformation tool to wield influence over Americans by pushing specific CCP-chosen content while hiding its source. Indeed, most young Americans today do not use TikTok simply to watch or "promote weird dance videos." *The Select: 'TikTok Special,' supra* (statement of Chairman Gallagher). To the contrary, TikTok is the "dominant news

platform for Americans under 30." *Id.*; *see also* TikTok.Br. 41. Given the CCP's external and internal influence over ByteDance and TikTok, the reliance by young people on TikTok for their daily news feed ensures that the CCP maintains editorial control over the content it gets tens of millions of American young people to consume every single day.

TikTok and ByteDance also have the power to boost certain videos and themes through their proprietary and confidential recommendation algorithm providing CCP officials yet another methodology for shaping the content seen and shared by American TikTok users. *See* Emily Baker-White, *TikTok's Secret 'Heating' Button Can Make Anyone Go Viral*, Forbes (Jan. 20, 2023), https://perma.cc/RW78-KTV9. For example, TikTok sent 170 million Americans a prompt encouraging them to call their representatives in Congress to oppose the very legislation before this Court. Maheshwari & McCabe, *supra*. This lobbying effort—created and driven by ByteDance, a CCP-proxy—prompted a "flood of phone calls" to congressional offices to oppose a purported "TikTok shutdown." *Id.* This example alone underscores how the CCP can deploy TikTok as a highly effective propaganda and misinformation tool to influence American policy debates.

Likewise, there is strong evidence that the TikTok content algorithm is built to effectuate the interests of the CCP and to limit content that might undermine its interests. For example, in 2023, the Network Contagion Research Institute released a report highlighting that the TikTok recommendation algorithm regularly down-prioritized content critical of the Chinese regime or supportive of the Hong Kong protestors. *A Tik-Tok-ing Timebomb*, NCRI and Rutgers Miller Center (Dec. 2023), https://perma.cc/4RFG-69RE; *see also* Fergus Ryan, et al., *TikTok and WeChat: Curating and Controlling Global Information Flows*, Australian Strategic Policy Institute (2020), https://perma.cc/K3SF-DH2H. Such decisions are not random and instead point to a concerted effort by TikTok and ByteDance to effectuate the CCP's goals and interests.

Similarly, the TikTok algorithm at times seeks to undermine American and allied interests. For example, in November 2023, in the aftermath of the horrific October 7 terrorist attacks conducted by Hamas in Israel, a flood of videos, one feeding off the other, praising Osama bin Laden's 2002 "Letter to America," were promoted across American feeds by the TikTok algorithm. *See* Donie O'Sullivan, et al., *Some young Americans on TikTok say they sympathize with Osama bin Laden*, CNN (Nov.

16, 2023), https://perma.cc/D6ST-9UL7. Without access to TikTok's proprietary algorithm, lawmakers questioned whether TikTok—controlled by the CCP—was affirmatively boosting the video. Alexander Ward & Matt Berg, *Why bin Laden's letter went viral on social media*, Politico (Nov. 16, 2023), https://perma.cc/4FSS-QYEW. Regardless whether TikTok affirmatively boosted the videos, two prominent Australian researchers recently explained that the Bin Laden incident demonstrates how "TikTok adds a force multiplier effect for disinformation [campaigns]" and noted that "[w]ith more than two billion TikTok users, a strategically crafted misinformation campaign can have a high chance of success," highlighting the "potential for [such videos]…to be[] a severe national security threat and have dangerous consequences." Sascha-Dominik (Dov) Bachmann & Dr. Mohiuddin Ahmed, *Bin Laden's "Letter to America": TikTok and Information Warfare*, Aus. Inst. of Int'l Affairs (Dec. 1, 2023), https://perma.cc/4Y5D-NGCH.

Each of these aspects of Chinese control over TikTok—the massive information gathering efforts, the internal pressure and control over company policy, the use of TikTok in combination with the fruits of CCP-coordinated hacking efforts, and the propaganda machine—is

independently problematic from a national security perspective. Together, they demonstrate that Chinese control of TikTok "poses a clear and present threat to America." *The Select: 'TikTok Special,' supra*.

II. The Act is a measured step to resolve the national security concerns posed by the Chinese government's control of TikTok.

The record here is "replete with evidence" of the national security harms posed by the Chinese government's ownership of TikTok. *See Heart of Atlanta Motel, Inc. v. United States*, 379 U.S. 241, 252 (1964); *Hamdi v. Rumsfeld*, 542 U.S. 507, 539 (2004). The Executive Branch and bipartisan majorities in Congress have highlighted these concerns and worked to address them directly. Because TikTok has failed to meaningfully address these concerns, Congress passed the Act, and the President signed it into law specifically to address the grave national security harms threatened by Chinese control over TikTok.

A. The political branches have flagged the national security concerns posed by Chinese control of TikTok.

The Executive Branch. The Executive Branch has been raising concerns about TikTok for years. In 2019, CFIUS reviewed ByteDance's acquisition of musical.ly, citing national security concerns. *President's Decision Regarding the Acquisition by ByteDance Ltd. of the U.S.*

Business of muical.ly, U.S. Dep't of Treasury (Aug. 14, 2020). Following this review, and pursuant to statutory authority, President Trump ordered ByteDance to divest certain assets "used to enable or support ByteDance's operation of the TikTok application in the United States." *Statement by Secretary Steven T. Mnuchin Regarding the Acquisition of Musical.ly by ByteDance Ltd.*, 85 Fed. Reg. 51297, 51297 (Aug. 14, 2020); *see also Addressing the Threat Posed by TikTok*, 85 Fed. Reg. 48637-38 (Aug. 6, 2020). In the Executive Order, the President described how TikTok's data collection "threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information." *Id.* at 48637. Specifically, the President explained that this data would allow "China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage." *Id.*

While President Biden revoked this Order in favor of taking other action, he continued to press the issues arising at the intersection of national security and data collection, including specifically addressing the threat posed by TikTok and ByteDance. *See Protecting Americans' Sensitive Data from Foreign Adversaries*, 86 Fed. Reg. 31423 (June 9, 2021).

Following the passage of legislation on the use of TikTok on government devices, White House rapidly implemented guidance to effectuate the removal of TikTok from government devices. *See* Memorandum for the Heads of Executive Departments and Agencies, *"No TikTok on Government Devices" Implementation Guidance*, OMB, M-23-13 (Feb. 27, 2023) (OMB TikTok Guidance); *see also* Pub. L. No. 117-328, div. R, §§ 101-02. The Administration also explained that it had "serious concerns" with TikTok and would continue to look "at other actions" it could take. *Press Gaggle by Principal Deputy Press Secretary Olivia Dalton*, White House Briefing Room (Feb. 28, 2023), https://perma.cc/92PD-SQ66. And shortly after TikTok was banned from government devices, President Biden stated that he would sign a bill banning TikTok altogether. *Remarks by President Biden Before Air Force One Departure*, White House Briefing Room (Mar. 8, 2024), https://perma.cc/58NG-4YAP.

Moreover, in his latest Executive Order regarding data collection issued less than six months ago, President Biden announced new proposals to regulate the type of data that "countries of concern," like China, have access to through applications like TikTok. *See Preventing Access to American's Bulk Sensitive Personal Data*, 89 Fed. Reg. 15780 (Feb. 28,

2024). The President specifically described how access to such data allows these countries of concern to engage in "malicious activities" like "espionage, influence, kinetic, or cyber operations." *Id.* at 15781. And under President Biden, the Department of Justice has continued to defend its authority over ByteDance and TikTok in the musical.ly acquisition before this Court. *See* Petition for Review, *TikTok Inc. v. CFIUS*, No. 20-1444, Doc. 1870778 (D.C. Cir. 2020).

Members of the Executive Branch have also repeatedly testified before Congress and warned the American public in detail about the grave national security threats posed by Chinese control of TikTok as well as ByteDance's direct links to the CCP. *See, e.g.*, *2023 Threat Assessment Hearing*, *supra*; *Homeland Security Secretary on TikTok's Security Threat*, Bloomberg (May 29, 2024) (interview with Secretary Mayorkas), https://perma.cc/W7PQ-68XH; *Fireside Chat with DNI Haines*, DNI Office (Dec. 3, 2022), https://perma.cc/L6AY-TL4D.[1] Between the Executive

[1] *See, e.g.*, *FBI Chief Says TikTok 'Screams' of US National Security Concerns*, Reuters (Mar. 9, 2023), https://perma.cc/F5WC-7AF3; Cecelia Smith-Schoenwalder, *5 Threats FBI Director Wray Warns the U.S. Should Be Worried About*, U.S. News (Jan. 31, 2024) (statement of Director Wray), https://perma.cc/D3B6-Y3UR.

Orders, testimony, and its public statements, as well as its filings in litigation brought by TikTok itself, the Executive Branch has repeatedly made clear its national security concerns regarding TikTok.[2]

Congress. Congress has likewise been quite direct and clear about its national security concerns. Elected officials from both sides of the aisle have expressed deep concerns with TikTok's data collection practices.[3] For example, Senator Warner (D-VA) and Senator Thune (R-SD) explained that TikTok can "enable surveillance by the Chinese Communist Party, or facilitate the spread of malign influence campaigns in the U.S." Press Release, *Senators Introduce Bipartisan Bill to tackle National Security Threats from Foreign Tech* (Mar. 7, 2023), https://perma.cc/X95L-4CD6. In the House of Representatives, Representative Gallagher (R-WI) and Representative Krishnamoorthi (D-IL) stated that "[s]o long as

---

[2] Independent agency leaders have express similar concerns. *See* Bethany Allen-Ebrahimian, *FCC commissioner says government should ban TikTok*, Axios (Nov. 1, 2022), https://perma.cc/WA2Y-XA76.

[3] *See, e.g.*, *Letter from TikTok Inc. to Senators Blumenthal and Blackburn* (June 16, 2023), perma.cc/4WXM-VR24; *Written Testimony of Geoffrey Cain on Social Media's Impact on Homeland Security*, U.S House of Representatives, Homeland Security and Governmental Affairs Committee (Sept. 14, 2022), https://perma.cc/UDW5-PWW4; *Deputy attorney general warns against using TikTok, citing data privacy*, ABCNews (Feb. 16, 2023), perma.cc/GKK7-BX9D.

[TikTok] is owned by ByteDance…TikTok poses critical threats to our national security." Press Release, *Gallagher, Bipartisan Coalition Introduce Legislation to Protect Americans from Foreign Adversary Controlled Applications, Including TikTok* (Mar. 5, 2024) ("*Gallagher Press Release*"), https://perma.cc/6NHJ-ZQCJ. Likewise, the Congressional Research Service has written several reports on the critical privacy and security issues in play with respect to TikTok.[4] And Congress held several hearings and briefings on the matter.[5] At these hearings, members of Congress, like Senator Rubio, expressed specific concerns about how the

[4] *See, e.g.*, *TikTok: Recent Data Privacy & Nat'l Security Concerns*, IN12131 (Mar. 29, 2023), https://perma.cc/9E94-3C25; *TikTok: Technology Overview & Issues*, R46543 (Updated June 30, 2023), https://perma.cc/U9SD-98EM; *Restricting TikTok (Part I): Legal History & Background*, LSB10940 (Updated Sept. 28, 2023), https://perma.cc/UV27-YBRL; *Restricting TikTok (Part II): Legislative Proposals & Considerations for Congress*, LSB10942 (Updated Mar. 15, 2024), https://perma.cc/PMW2-2QUB; *TikTok: Frequently Asked Questions & Issues for Congress*, R48023 (Apr. 9, 2024), https://perma.cc/U2Q8-3L3N.

[5] *See, e.g.*, *2023 Threat Assessment Hearing* at 1:09:00, *supra*; *Testimony of Shou Chew*, H. Comm. on Energy & Commerce, No. 118-13, 118th Cong., 1st Sess. (Mar. 23, 2023), https://perma.cc/6G5S-K77A; *Hearing Memorandum*, H. Comm. on Energy & Commerce, No. 118-13, 118th Cong., 1st Sess. (Mar. 20, 2023), https://perma.cc/3EV6-7AZA; *2023 House Data Privacy Hearing*, *supra*; *Protecting Americans from Foreign Adversary Controlled Applications*, H. Rep. 118-417, 118th Cong., 2d Sess. 1 (Mar. 11, 2024), https://perma.cc/9S3H-GME8.

CCP manipulates information fed through TikTok and argued that the application "is probably one of the most valuable surveillance tools on the planet." *2023 Threat Assessment Hearing* at 1:09:00, *supra*.

Indeed, it was concerns about the CCP and its activities targeting Americans that convinced the House of Representatives to establish the Select Committee on Strategic Competition between the United States and the CCP. The China Select Committee, as it is colloquially known, has repeatedly sounded the alarm over the national security threat posed by TikTok. *See, e.g., Rep. Gallagher Letter*, *supra*. Specifically, the China Select Committee has noted that "the Chinese Communist Party—and its leader Xi Jinping, have their hands deep in the inner workings of" TikTok," explaining that ByteDance "is legally required to support the work of the Chinese Communist Party." *See Press Conference to Introduce the Protecting Americans from Foreign Adversary Controlled Applications Act*, China Select Committee (Mar. 6, 2024) (statement of Chairman Gallagher), https://perma.cc/NBC3-H3PB.[6] Likewise, during a China

[6] The States, too, have long been investigating TikTok under their consumer and child protection laws, police powers, and their authority to protect state systems and critical infrastructure. *See, e.g.*, David Shepardson, *State AGs demand TikTok comply with US consumer protection*

Select Committee hearing to discuss the CCP's support for America's adversaries, former Secretary Pompeo described TikTok as engaging in "information warfare" because it delivers different content to Americans than it does to individuals in China. *See Transcript of Hearing on Authoritarian Alignment*, China Select Committee (Jan. 30, 2024), https://perma.cc/XQD2-578Z.

B. TikTok has failed to respond to these legitimate concerns.

Despite these public concerns, TikTok itself has repeatedly failed to effectively address legitimate questions from Congress and others on how it collects, stores, and shares data, including sensitive personal data of Americans. *See 2023 House Data Privacy Hearing*, *supra*. And the fact

---

investigations, Reuters (Mar. 6, 2023), perma.cc/9NL6-2VPW; Justine McDaniel, *Indiana sues TikTok, claiming it exposes children to harmful content*, Washington Post (Dec. 7, 2022), perma.cc/V2RV-AU3P; *see also, e.g.*, *ICYMI: Attorney General Austin Knudsen Joined Krach Institute to Discuss Montana's TikTok Ban and Chinese Spy Balloon*, Montana Dep't of Justice (Sept. 28, 2023), https://perma.cc/UN8H-2ZNL; *Attorney General Miyares Leads 18 State Coalition Supporting Montana's TikTok Ban*, Office of the Virginia Attorney General (Sept. 19, 2023), https://perma.cc/27R8-2DAY. Indeed, as of March 2024, thirty-nine States have barred TikTok from government devices, citing concerns about the security of state and critical infrastructure systems as well as state government data. *See* Cailey Gleeson, *These 39 States Already Ban TikTok From Government Devices*, Forbes (Mar. 12, 2024), https://perma.cc/T7Y4-XJY9.

that China "has made clear in public statements that it would not permit a forced divestment," only reinforces these concerns. TikTok.Br. 2.

For example, at a congressional hearing last year, TikTok's CEO acknowledged that some China-based employees continue to have access to U.S. data, including sensitive personal data of Americans. Lauren Feiner, *TikTok CEO says China-based ByteDance employees still have access to some U.S. data*, CNBC (Mar. 23, 2023), https://perma.cc/9LU9-JBAN. Moreover, when pressed, TikTok's CEO could not say whether TikTok sells data to other entities or whether the Chinese government exerts influence over TikTok. *See* Louis Casiano & Hillary Vaugh, *TikTok CEO refuses to answer if Chinese government has influence over platform as Congress mulls ban*, Fox Business (Mar. 14, 2024), https://perma.cc/8BCT-ERTL; Ken Tran & Rachel Looker, *What does TikTok do with your data?*, USA Today (Mar. 23, 2023), https://perma.cc/2LVQ-3Z6L. And when asked whether ByteDance has an internal CCP committee, the TikTok CEO punted, responding, "[l]ike I said, all businesses that operate in China have to follow the law." *See* D. Wallace, *TikTok CEO grilled on Chinese Communist Party influence*, Fox Business (Jan. 31, 2024), https://perma.cc/KJ9F-8HJ7. The inability

of senior TikTok leaders to effectively allay the basic concerns of American lawmakers only reinforces the pervasive and unique threat that TikTok poses to Americans and our national security.

C. Project Texas does not mitigate the risks or address the ongoing harms.

Finally, TikTok's efforts to appease U.S. lawmakers through a plan to retain American data wholly in the United States (aka "Project Texas") have likewise failed to meaningfully eliminate key national security concerns. While the physical location of data storage for American user may conceivably alleviate *some* concerns, what really matters is the "leverage" China "has over the people who have access to that data." *See* D. Harwell & T. Room, *Inside TikTok*, Washington Post (Nov. 5, 2019), https://perma.cc/B368-JNN4 . Contrary to TikTok's claims about how Project Texas would protect American data and limit the threat posed to Americans from potential disinformation efforts, TikTok's own repeated statements reveal that the CCP continues to have access to user data stored in America and exercises deep influence on—and control over—TikTok's internal decision making. Indeed, TikTok "[m]anagers told employees that they actually could save data to their computers, and that there would be exceptions" to Project Texas's data sharing restrictions.

Georgia Wells, *TikTok Struggles to Protect U.S. Data from Its China Parent*, WSJ (Jan. 30, 2024), https://archive.is/a8LtA.

As long as TikTok continues to use its own algorithm—developed and managed in China—the CCP is bound to be able to access data, regardless where it is stored. As one TikTok employee stated, "[i]t remains to be seen if at some point product and engineering can still figure out how to get access, because in the end of the day, it's their tools." *See* Emily Baker-White, *Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China*, Buzzfeed (June 17, 2022), https://perma.cc/7LF4-Y3XD. Indeed, while Project Texas may look good on paper, former employees have said the project has been mostly "cosmetic" and has failed to address the core concerns over the application and CCP access to American data. *See* Gaby Del Valle, *Report: TikTok's effort to silo US data 'largely cosmetic'*, The Verge (Apr. 16, 2024), https://perma.cc/WR45-NZCU.

In sum, after months of digging deep into TikTok and its operations, it was clear to key Congressional leaders that TikTok fundamentally functions as an arm of the CCP in both promoting and censoring data in the interests of the CCP. And because TikTok fails to meaningfully

address the national security concerns, Congress was forced to step in and take action.

D. Congress passed the Act to resolve the national security concerns posed by Chinese control of TikTok.

The Act addresses these precise concerns. In March 2024, the bipartisan leadership of the China Select Committee, along with other key members of the House, introduced legislation that became the genesis for the legislation challenged in this matter. *See* Pub. L. No. 118-50, div. H, 138 Stat. 955 (2024); *see also Gallagher Press Release*, *supra*. Relying on the extensive record built over the preceding months as it conducted its deep dive into the national security threat posed by TikTok, the legislation—which was incorporated into a foreign aid package—easily passed the House and Senate. Roll Call 145: H.R. 8038, Clerk of the United States House of Representatives, 118th Cong.(Apr. 20, 2024) (passing the House with a vote of 360-58); Roll Call 154: H.R. 815, United States Senate, 118th Cong. (Apr. 23, 2024) (passing the Senate with a vote of 79-18). President Biden signed the bill into law the following morning. *See* H.R. 815, 118th Cong., Congress.gov (Apr. 24, 2024). This legislation—which only requires divestment by ByteDance of the TikTok application—and does not effectuate any restrictions on TikTok's availability if

divestiture happens—is a measured and sensible response to the national security threat posed by TikTok. *See* Pub. L. No. 118-50.

III. The government's compelling national security interests overcome any applicable level of First Amendment scrutiny.

Having failed to effectively confront the enduring national security threat that TikTok and its relationship with the CCP poses to American's and their data, TikTok now seeks to wrap itself in the American flag, citing the First Amendment as the core reason the government ought not be able to force divestiture. *See* TikTok.Br. 28-38. However, as the United States correctly explains, the Act does not even implicate the First Amendment. *See* USA.Br. 59. This is because the Act doesn't target *any protected speech* nor a*nyone with free speech rights*. Rather, it targets the CCP's control of TikTok, and requires divestiture by its Chinese owners if TikTok is to continue to enjoy unabated access to the sensitive personal data of over 170 million Americans. See USA.Br. 1-3. Contrary to TikTok and ByteDance's claims that there is something unique or untoward going on here, the federal government has long regulated foreign ownership and control of companies operating in all sorts of industries. *See, e.g.*, 12 U.S.C. §72 (nationally chartered banks); 16 U.S.C. §797 (dams, reservoirs, and similar projects); 42 U.S.C. §§2131-34 (nuclear facilities); 49

U.S.C. §§ 40102(a)(15), 41102(a) (air carriers). Indeed, the federal government has long regulated foreign ownership telecommunications assets and media, including radio and broadcast television licenses, for nearly identical reasons. 47 U.S.C. § 310(b)(3) (radio and broadcast television); *see Pacific Networks Corp. v. FCC*, 77 F.4th 1160 (D.C. Cir. 2023). In *Pacific Networks*, just last year, this Court upheld the FCC's revocation of authorizations for Chinese telecommunications companies to operate communications lines in the United States because Chinese control of such companies "provid[ed] opportunities for … the Chinese government to access, monitor, store, and in some cases disrupt [or] misroute U.S. communications, which in turn allow them to engage in espionage and other harmful activities against the United States." *Id.* at 1162-63; *see also China Telecom (Americas) Corp. v. FCC*, 57 F.4th 256, 265-66 (D.C. Cir. 2022).

Moreover, even if there is some expressive content on the TikTok platform that would be adversely affected by a required divesture—although TikTok fails to explain what such content might be—Congress can regulate TikTok's pervasive and widespread collection of Americans' personal data, which is not itself expressive activity. *See Sorrell v. IMS*

Health, Inc., 564 U.S. 552, 567 (2011) ("[T]he First Amendment does not prevent restrictions direct at commerce or conduct from imposing incidental burdens on speech."); *Haig v. Agee*, 454 U.S. 280, 307 (1981) ("[N]o governmental interest is more compelling than the security of the Nation."). And even if TikTok's recommendation algorithm might be viewed as having some expressive function, in that it ostensibly engages in an editorial function by curating content, such speech is unprotected because it is the speech of foreign entities—ByteDance, TikTok Global, and the CCP—none of whom are entitled to First Amendment protection. *See Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc.*, 591 U.S. 430, 436 (2020) ("[P]laintiffs' foreign affiliates possess no rights under the First Amendment."); *see* USA.Br. 59-60. And while TikTok US may be incorporated in the United States, TikTok has made clear that the technology fueling its algorithm is developed in China and is ultimately controlled by its Chinese parent company, ByteDance, which, in turn, faces inexorable pressure—and control—by the CCP. *See* TikTok.Br. 24. Nothing in the First Amendment can be read to shield the covert influence or intelligence collection efforts of a foreign government targeting the American people.

The only even *arguably* protected speech that might even *theoretically* be affected is that of American content creators and (perhaps) any content moderation performed by TikTok US that is done completely separate and apart from TikTok's CCP-dominated recommendation algorithm. There are, of course, a number of reasons why this theoretical impact is not actionable. First, speech rights are personal and cannot be raised vicariously by others as TikTok seeks to do in this litigation. *Broadrick v. Oklahoma*, 413 U.S. 601, 610-11 (1973); *see also Murthy v. Missouri*, 144 S. Ct. 1972, 1996 (2024). Second, TikTok has repeatedly made clear that its content moderation is driven primarily by the core TikTok algorithm, which is not only built in and controlled by Chinese entities but is actually significantly responsive to the goals and interests of the CCP. *See, e.g.*, *A Tik-Tok-ing Timebomb: How TikTok's Global Platform Anomalies Align with the Chinese Communist Party's Geostrategic Objectives*, NCRI and Rutgers Miller Center (Dec. 2023), https://perma.cc/4RFG-69RE; *see also* Fergus Ryan, *supra*. Third, to the extent content creators present in this litigation might validly raise their own First Amendment claims, the fact is that while the First Amendment may protect relevant expressive activity and content, it does not

guarantee a particular venue for such speech—particularly when the venue is a private forum, not a public space controlled by the government—and even where it is, the government can impose in reasonable content-neutral time, place, and manner restrictions so long as they are content-neutral. *See Heffron v. International Soc'y for Krishna Consciousness, Inc.*, 452 U.S. 640, 647 (1981); *Kovacs v. Cooper*, 336 U.S. 77, 88-89 (1949). And finally, the availability of a wide and diverse range of alternative venues for American speech—from Instagram to YouTube and beyond—must weigh into any analysis of the claimed infringement of speech rights. *See, e.g.*, *Ward v. Rock Against Racism*, 491 U.S. 781, 802 (1989).

And even if these issues were not themselves insurmountable barriers to TikTok's failed effort to hide behind the U.S. Constitution, the fact that the Act doesn't actually inhibit *any* speech is just such a barrier. Rather than barring speech, as the government correctly points out, "Congress expressly authorized the continuation of [] expressive activities on TikTok so long as the national-security harms could be mitigated." *See* USA.Br. 60.

The Act thus has only an incidental—if any—impact on arguably protected speech. Under longstanding precedent, the Act is therefore lawful so long as it is "within the constitutional power of the Government [and] furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." *United States v. O'Brien*, 391 U.S. 367, 377 (1968).

The Act easily meets this test. To begin with, the Framers understood national security to be the "principal purpose[]" of government. The Federalist No. 23 (Alexander Hamilton); *see also* Federalist Nos. 34, 41. The Constitution therefore confers upon Congress robust national-security authority, *see, e.g.*, U.S. Const. art. I, §8, cl. 3, 11, 12, 13 (to regulate foreign commerce, declare war, raise and support armies and the Navy), and vests the President with "[t]he executive Power," establishes him as the "Commander in Chief," *id.* art. II, §1 & §2, cl.1, and making him the Nation's "'sole organ'" in foreign affairs. *Zivotofsky ex rel. Zivotofsky v. Kerry*, 576 U.S. 1, 20 (2015) (quoting *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936)).

And as the examples above illustrate, *see supra* at 20-21, it is well established that regulating foreign ownership and control of companies operating within the United States—particularly in the media and telecommunications industries—is within the scope of these broad powers. The Act thus falls safely "within the constitutional power of the Government." *O'Brien*, 391 U.S. at 377. Further, the government's national security interest in preventing "the national-security harms that accompany China's ability to exploit TikTok," USA.Br. 59, is "unrelated to the suppression of free expression," *O'Brien*, 391 U.S. at 377, especially because, as noted above, the Act requires divestment of TikTok and nothing more. For the same reason, any incidental burden on protected speech is no "greater than is essential to the furtherance of [the Government's national security] interest," *id.*, especially because "[a]ny TikTok users in the U.S." who might feel some incidental burden on their speech "have the option of turning to other platforms." *See* USA.Br. 60; *see Heffron*, 452 U.S. at 647 ("[T]he First Amendment does not guarantee the right to communicate one's views at all times and places or in any manner that may be desired.").

This is the case regardless of what level of First Amendment scrutiny might be applied. The Act's divestment remedy is narrowly tailored to address the specific national security harms threatened by Chinese control of TikTok as well the government's interest in protecting more than 170 million Americans from the theft and misuse of their sensitive personal data by proxies of a foreign nation-state and the CCP's covert influence efforts. These matters are not simply *a* compelling interest, but perhaps *the most* compelling interest. *See Haig*, 453 U.S. at 307.

CONCLUSION

For these reasons, the petitions should be denied.

Dated: August 2, 2024

Respectfully submitted,

/s/ Thomas R. McCarthy
Thomas R. McCarthy
Kathleen S. Lane
Consovoy McCarthy PLLC
1600 Wilson Boulevard, Suite 700
Arlington, VA 22209
(703) 243-9423
tom@consovoymccarthy.com
katie@consovoymccarthy.com

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limit of Federal Rule of Appellate Procedure 29(a)(5) because it contains 6,497 words. This brief also complies with the typeface and type-style requirements of Federal Rule of Appellate Procedure 32(a)(5)–(6) because it was prepared using Microsoft Word in Century Schoolbook 14-point font, a proportionally spaced typeface.

Dated: August 2, 2024

/s/ Thomas R. McCarthy
Thomas R. McCarthy

Counsel for Amici Curiae

APPENDIX A: LIST OF AMICI CURIAE

The Hon. Michael B. Mukasey
Former Attorney General of the United States
Former Judge, United States District Court for the Southern District of New York

The Hon. Jeff Sessions
Former Attorney General of the United States
Former United States Senator

The Hon. Chris Inglis
Former National Cyber Director, The White House
Former Deputy Director, National Security Agency

The Hon. Christopher A. Ford
Former Assistant Secretary of State for International Security & Non-proliferation, United States Department of State
Former Senior Director for Weapons of Mass Destruction & Counterproliferation, National Security Council, The White House

The Hon. Michelle Van Cleave
Former National Counterintelligence Executive, Office of the Director of National Intelligence
Former General Counsel and Assistant Director, Office of Science and Technology Policy, The White House

The Hon. William Evanina
Former Director, National Counterintelligence and Security Center

Gus P. Coldebella
Former General Counsel (acting), United States Department of Homeland Security

Margaret M. Peterlin
Former Chief of Staff to the Secretary of State, United States Department of State

Former National Security Advisor to the Speaker of the House, United States House of Representatives

Vice Admiral (Ret.) Mike LeFever
Former Director of Strategic Operational Planning, National Counterterrorism Center, Office of the Director of National Intelligence
Former Commander of the Office of Defense Representative in Pakistan & Commander of the Joint Task Force in Pakistan

Norman T. Roule
Former National Intelligence Manager for Iran, Office of the Director of National Intelligence
Former Division Chief, Central Intelligence Agency

Dr. Lenora P. Gant
Former Assistant Deputy Director of National Intelligence for Human Capital, Office of the Director of National Intelligence
Former Senior Executive for Academic Outreach and Science, Technology, Engineering, and Mathematics & Senior Advisor to the Research Directorate, National Geospatial-Intelligence Agency

Paula Doyle
Former Associate Deputy Director for Operations Technology, Central Intelligence Agency
Former Deputy National Counterintelligence Executive, Office of the Director of National Intelligence

Teresa H. Shea
Former Signals Intelligence Director, National Security Agency

Michael Geffroy
Former General Counsel, Senate Select Committee on Intelligence, United States Senate
Former Deputy Chief of Staff and Chief Counsel, Committee on Homeland Security, United States House of Representatives

Geof Kahn
Former Senior Advisor to the Director of Central Intelligence, Central Intelligence Agency
Former Policy Director & CIA Program Monitor, House Permanent Select Committee on Intelligence, United States House of Representatives

Jamil N. Jaffer
Former Chief Counsel & Senior Advisor, Senate Foreign Relations Committee, United States Senate
Former Associate Counsel to President George W. Bush, The White House

Rick "Ozzie" Nelson
Former Director, Joint Interagency Task Force, Joint Special Operations Command
Former Group Chief, National Counterterrorism Center

Andrew Borene
Former Senior Officer, Office of the Director of National Intelligence
Former Associate Deputy General Counsel, Department of Defense

Edward Fishman
Former Member, Policy Planning Staff, Office of the Secretary of State, United States Department of State
Former Russia and Europe Sanctions Lead, United States Department of State

Senator VAN HOLLEN. Well, thank you, and thank all of you for your testimony.

And just picking up on one of the points you raised, we have had bipartisan support to try to provide substitutes—competitive substitutes to Huawei and ZTE for the reasons that you explained—rip and replace here at home. But we need to continue to be vigilant on a bipartisan basis and provide alternatives to these countries.

Let me just focus first with you, Ms. Cunningham, because we are trying to use this hearing to identify things that we can do to try to break through censorship, like the firewalls in China and other places, and as Senator Romney said, in many cases, as you know, this is a race against technology.

But there are also ways we can raise costs on both countries and companies that are engaged in this kind of activity or aiding and embedding this kind of activity.

You know, back in the day during the cold war we had Radio Free Europe, Radio Liberty, to try to, you know, overcome censorship in the Soviet Union. There were always efforts to jam those radio signals. We are on to new technologies right now.

So just focusing now on technology, if you could talk a little bit about how you all at the OTF are helping dissidents and others in countries that have extreme censorship to try to use technology so they can get good information about what is happening in their countries and elsewhere around the world.

Ms. CUNNINGHAM. Thank you.

The Open Technology Fund invests in two categories of technology—anti-censorship tools like VPNs that the chairman has already spoken about, as well as privacy and security enhancing technologies to make sure that civil society and journalists around the world are able to stay safe and report safely during their work.

The challenge here is that we are just woefully outspent when it comes to innovating and supporting these technologies.

In just the last 2 years demand for OTF supported VPNs has increased by over 500 percent, and we do not have the resources to support the VPN users around the world who are eager for these tools, who want to access free and independent information.

The challenge, frankly, on that front is not a technical one. We have VPNs that work well, that are secure and effective, but we just do not have the resources to be able to meet the demand for users around the world who are facing online censorship for the very first time.

It is also critically important to your point, Mr. Chairman, that these tools are there to help get free and independent news and information to citizens around the world. We actually work very closely with Radio Free Europe, including Radio Farda, which works in Iran. We know that our VPNs deliver 90 percent of their Farsi audience to Radio Farda.

So these tools are not only effective, they are being used to seek out and find the exact type of information that we want dissidents—that we want human rights defenders to find.

However, as I said, the challenge right now is resources. When we are competing with China and Iran, who are spending billions

of dollars on these technologies, it is hard with only millions to be able to meet the accelerating demand we see around the world.

Senator VAN HOLLEN. So it sounds to me like your answer is we do have the technological wherewithal to break through some of these censorship walls, but it is a question of resources. Let me also ask you about the role of sort of private internet service companies and others in these spaces.

So, for example, in China U.S. social media companies do not—they cannot operate there consistent with the rules. Of course, China has a wide open access to markets in the United States and elsewhere around the world.

But in many of these places there are internet service providers and other private companies that are aiding and abetting authoritarian regimes.

So maybe you could identify some of those examples and what we can do to raise the cost on those private sector companies that are essentially colluding with those foreign governments that are trying to oppress the people and deny them access to important information.

Ms. CUNNINGHAM. I think this is one of the most critical challenges that we face in China right now in particular, is U.S. private sector technology companies' complicity with Chinese government censorship.

An example that comes to mind for me is the Apple App Store. We know that at the request of the Chinese government Apple has removed independent news and information apps like Radio Free Asia, for example, from the Apple App Store in China, preventing Chinese citizens from accessing that information.

But they have gone further than that. They also remove, based on requests from the Chinese government, most internet freedom technologies. So if you are a Chinese citizen in China you cannot access the VPNs that I just described.

You cannot access the secure information and communication technologies that the U.S. Government is supporting because Apple is actively removing them from the App Store.

Finding ways to increase both the transparency and cost for those companies to remove U.S. funded internet freedom technologies, but also independent news and information, is critical in ensuring that Chinese citizens can continue to access this information.

Senator VAN HOLLEN. I appreciate your raising that example, and we are looking at ways to address it. We need to also make sure that if, for example, another company comes in and just replaces Apple that they do not get the benefit of that market share without being somehow penalized from their entry into other markets. So thank you for raising those issues.

Senator Romney.

Senator ROMNEY. Thank you, Mr. Chairman, and thank you to the individuals who have spoken with us this morning.

I would imagine that if I were an authoritarian like Xi Jinping I would use these tools exactly the way he is doing them. I would use them to spy on people, to spy on the United States, to spy on my adversaries.

I would use them to censor the news to make sure they only got what supported me and my continuation as the leader of China.

So when I hear discussion of we need to establish norms and let them know they are breaking norms or an expression of, what was it, an expression of concern by the U.S. Senate, if I were Xi Jinping I would laugh.

It is, like, who the heck cares about global norms or expressions of concern of the United States and the Senate? The only thing that would allow us to defeat the spread of authoritarianism and digital authoritarianism is by having the tools and capabilities to push back against it and exercising our own strength.

Am I wrong in that assessment? I mean, It just strikes me—I will turn to you, Mr. Jaffer. It strikes me that the pathway for us is to lead in technology, to push back against the Huaweis.

I mean, to eliminate the Huaweis from our systems and TikTok from our system, get them out, and then work to help replace them in other places, and to have the rest of the world recognize this is a battle between freedom and authoritarianism, and they are going to do all these things because our norms they laugh at, and their norms we find reprehensible, but that is where we are.

Am I wrong? And I applaud the work that you are doing to provide additional sources for information. But I look at what the Russians are doing and the Chinese, but particularly the Russians with all their bots overwhelming our systems. They are so far ahead of us in these things. That is one more that I would take on.

But Mr. Jaffer, help me on this. It strikes me that most of what we are talking about just does not make sense unless it is, hey, stay ahead of them—use our technology to identify them and kick them out.

Mr. JAFFER. No, Senator Romney, you are exactly right. The idea of sort of strongly worded letters from the Senate or from our diplomats or the like are not going to get this job done.

What is going to get this job done is providing people who want freedom in those countries access to news and information the way that the Open Technology Fund is doing, and ensuring that we are investing here at home, that we are building the best and most awesome technology here at home.

I mean, look, if you look around the world today, we are the leaders in AI, but that position is not guaranteed. In fact, if we adopt the approach the Europeans have taken, which is regulate, regulate, and regulate, right, we are likely to lose that edge.

So we need to avoid over regulation here. We need to incentivize investors here in the United States and innovators here in the United States. You know, there is a reason why the world wants to come here to the United States.

It is because we have the most productive system of the allocation of capital around the globe, and protecting and preserving economic liberty is critical to the effort to fight authoritarianism around the globe, right.

It is not just that we are going to have a freedom of societies. We have got to take advantage of it, double down on it, and that is why also ensuring that our investors are not investing in Russia, in China, in Iran, and North Korea—all too many American inves-

tors take the benefit of investing in China and getting that advantage.

But the truth is those investments are terrible. Those investments ultimately lose money, and in the long run the right approach is to invest here, invest in our allies, and invest in trust, safety, and security.

And so we believe that there actually is an investment thesis around investing in the U.S. Senator Ricketts, you are an innovator. You have worked in this space. You have helped develop startups.

Senator Romney, you have done this at Bain for a decade. That is what it is about. It is about the allocation of capital, and until we recognize that all too many Europeans and the European system views us as the enemy, views our technology companies as the enemy, when in fact we are actually the innovators who are creating this space and these opportunities, I think, at the end of the day, what we have got to do to your point, Senator Romney, is double down on that and avoid the strongly worded letters.

And the last point I will make is if we are worried about what is happening in cyber domain, the best and most effective way to succeed in the cyber domain is to push back against what Russia, China, and Iran are doing, and until we respond to their activities here in our country attacking us and our allies, they are not going to get the message.

Senator ROMNEY. I have not got quite enough time to turn to the next question, but I got to try it nonetheless.

Please be brief because I took a long time, and that is and I guess I will do it in the second round. I am looking—I have got 19 seconds. So I am not—that is not fair to you, Ms. Cunningham. We will come back and address in a moment. Thank you.

Mr. JAFFER. Apologies. I think I used up too much of your time, Senator. I apologize.

Senator VAN HOLLEN. To the newest member of our committee, Senator Helmy.

Senator HELMY. Thank you, Chairman.

I would start by thanking you and the ranking member and this committee for the work it has done and the legacy you both in this committee have. You have taken a global competitiveness and security issue, and from my experience in financial services, health care and state government, the work that this committee does on the global level has had real impacts, as Mr. Jaffer mentioned, to the work that state governments do to better prepare for the global threat and our critical institutions like health care, utilities, and otherwise.

Mr. Jaffer, I am going to pull on a string you left in your testimony there, if I may, and to the ranking member's question.

It is clear that the U.S. Government has much ground to cover to compete with the PRC in technological innovation. You have mentioned the need for additional capital, which would include more robust funding for research and development to emerging technologies, cross-collaboration with the private tech sector as a means of advancing our interest in national security in the cyberspace.

How do you envision the U.S. cyber deterrence strategy when the legal parameters and international norms do not address the current bad behavior of our adversaries, including the PRC and Russia?

Mr. JAFFER. Thank you, Senator Helmy.

Look, I think that today the level of activity we have seen on American systems is sufficient to enable us to push back if we wanted to, and that pushback can come in the form of cyber options, or it can also come in the form of other options—sanctions and the like.

Today, America's intellectual property has been stolen to the tune of billions of dollars a year, trillions total, and as a result, that damage alone to our economy and the threat it poses to our national security is enough to warrant more aggressive active pushback in the cyber domain.

I think the norms are there. We are choosing not to take advantage of them.

Senator HELMY. Thank you.

Mr. Kaye, in light of the upcoming election the subcommittee's work, obviously, is going to pivot on the critical response to enduring the challenge of curtailing authoritarian regimes that seem to have no constraint on their digital oppression at home and their efforts abroad.

What hopes do you have for future Administrations to properly address the use of commercial spyware, particularly by our authoritarian adversaries?

Mr. KAYE. Thank you for that question, Senator Helmy, and that also gives me an opportunity to respond in part to Senator Romney's point.

So I want to make two points here. The first is that although I share the concern very much about Chinese repression at home and its export of its repression abroad, I think it is important to see the moment that we are facing as a moment in which we have a very cheap availability of tools that are spreading well beyond the states that have that kind of power.

And so there is a range of steps actually that the Congress has already been taking actually at a normative and at an operational level, let us say, to deal with the threat of foreign commercial spyware, and I think that is actually important, and there is quite a bit to build on there.

The second point that I wanted to make is maybe to give it defensive norms for a moment because I do think that while there is a kind of battle in the trenches right now that is a technology battle and is also a geopolitical battle, it is also a normative battle, and that normative battle is a vision of a free and open internet on the one side, the one that I think we all share, and a vision of one that is all about state control.

And it is not just a question of those norms being adopted by U.N. resolutions and so forth. It is a question of those norms being essentially embedded in our laws and the Congress and the State Department and others pushing for those norms to be a part of our allies' laws, so that their own use of this technology and their own export of the technology is constrained by rules.

So I see a connection between norms, which I agree in the abstract do not mean that much, but norms that are actually operationalized, I think there is quite a bit of room, and there is actually quite a bit to build on from both what Congress has done and what the Biden administration has done in recent years.

Senator HELMY. Thank you, Mr. Kaye. That concludes my questions.

Thank you, Chairman.

Senator VAN HOLLEN. Thank you.

Senator Ricketts.

Senator RICKETTS. Thank you, Mr. Chairman.

The use of cyber warfare both in peacetime and armed conflict has become a reality. Over the last 20 years Russia has developed its capabilities, trained its hackers, advanced its capacity to undertake a wide range of cyber operations.

Since Russia's illegal invasion of Ukraine Russian hackers have breached Ukrainian telecom systems and executed multiple cyber attacks on the Ukrainian government.

Despite these efforts, Ukraine has proven resilient. While the odds seem to favor Russia's dominance in cyberspace, they have not prevailed against Ukraine, and Ukraine has largely maintained its presence online.

Banks remained operational. Lights have remained on, unlike the cyber attacks of 2015 and 2016 that caused blackouts, electricity and information—you know, electricity and information continue to flow.

While Russia possesses the means and capabilities and the intent to cripple Ukraine's cyberspace and critical infrastructure, the reality has been different. Their efforts have not been successful.

So, Mr. Jaffer, why has Russia not succeeded? Why have they not been able to bring Ukraine to its knees from cyber attacks and turn off the power and so forth?

What do you attribute Ukraine's success to?

Mr. JAFFER. Well, I think a few things, Senator Ricketts.

One, I think that we did do a lot of work ahead of time working with Ukraine to get it stronger, get it more defensible.

A lot of the capabilities Ukrainians are deploying today are American technologies built by American technology companies that have been hardened against these type of Russian attacks. So that is one, I think, answer to why Russia has been less successful than we would hope.

I think the second piece of it is, frankly, that the Russians have not embedded as deep as they might have in the Ukrainian networks and delivered the capabilities they could have delivered early on in this conflict, and so Ukraine was able to get their stuff out more rapidly than I think the Russians expected.

It is true in the physical world, and it has been true in the cyber world as well. I think there is a lesson for that—for the United States.

We rely so much on our technological networks that we can identify ahead of time if the individual—if the private sector and public sector, are able to partner effectively we too can defend ourselves against these type of threats in a more effective way than we are today.

Senator RICKETTS. So, I am interested by what you said there about being embedded. Is this something where Russia was not looking at Ukraine as much as maybe they are looking at the United States? Or is there a lesson here for us with regard to what else we need to be doing with regard to rethinking our cyber strategies?

Mr. JAFFER. Well, I think that we know how deep the Russians and the Chinese are in our networks. Just over the past year we have heard a lot about how deep the Chinese have gotten and the fact that they are deploying actual disruptive and destructive capabilities in American systems through this Volt Typhoon set of attacks.

So we know that they are doing it. We know that they are getting in place. Now, whether the Russians deploy those kind of capabilities, which we know they have, as deep in the Ukrainian networks or not is unclear. They clearly did not use them.

We have seen the Russians use destructive attacks in the past. We know they have the ability to wipe out systems.

So I think the answer here is twofold. One, when we identify these capabilities in our networks we have got to get them out.

We have got to deter them from putting them in in the first place, which we are not doing effectively because we are not really pushing back against Russian, Chinese, Iranian, and North Korean attacks.

And then, finally, I think what the Ukrainians did effectively, which we still need to do more of in this country, is to partner between the public and private sectors to ensure that their systems are more defensible. We want to do that here in the United States.

We are just not been—not very good at it. We have tried for a decade. We need to get better at that and fast.

Senator RICKETTS. So we talked about what we can learn from this. What do you think our adversaries are learning from this, based upon Russia, what they have done in Ukraine and what they have not actually been able to get done in Ukraine?

Mr. JAFFER. Yes. As we think about China and a potential Taiwan scenario I think what they are looking at is if you are going to go in make sure you have the capabilities you need both on the ground and cyber wise, and do not go in until you can finish that conflict in a week.

We thought it would be over in a week when the Russians invaded Ukraine. The Ukrainians were able to push back aggressively and hold the line and have held the line now for the better part of 2 years.

So I think what our adversaries are learning is you got to get in. You got to get deep. You have to know your capabilities are there and then effectuate them, and that is why I think the Russian—I think that is why the Chinese are waiting, for instance, on Taiwan.

They are not waiting because they are scared of us. We are not there. We cannot get there in time to stop them. If we do not position stuff forward, we will never win that fight and they know it.

So they are not waiting for us. They are waiting because they are not ready to go in fully, and I think that is a lesson they are learning from Ukraine.

Senator RICKETTS. But specifically on the cyber aspect of it you think that what they are learning is they have to be deeper into the networks?

Like, Russia should have been deeper into Ukraine's networks before they launched this attack, and you think that that is what the PRC is learning about Taiwan, that maybe they do not feel like they are deep enough into Taiwan's networks before they could be successful in executing some of these cyber attacks?

Mr. JAFFER. I think that is exactly it.

Taiwan and our networks, because they want to be able to push back against us so that if in fact we were to intervene on behalf of Taiwan, they could cripple us as well.

They know that is their strategic advantage. That is what they are looking to do, and that is why Volt Typhoon and the change in Chinese behavior that we have seen in the last 6 months is so critical to focus on.

Senator RICKETTS. Great.

So OK, I am down to 2 seconds too, so I am going to turn it back over to the chairman. But thank you very much, Mr. Jamil.

Senator VAN HOLLEN. Thank you, Senator Ricketts.

So in my initial questioning I was focused on how we try to break through the censorship firewalls in places like China, places like Iran, Russia now. But if we look at the commercial spyware market, it is not necessarily those countries who are the most advanced in developing these technologies.

So, Mr. Kaye, I would like to focus on that issue for a moment, because groups like the University of Toronto Citizen Lab, Amnesty International, and Access Now have documented the targeting of Russian and Belarusian speaking civil society and media figures residing in exile in Europe, civil society figures in Jordan, journalists and human rights defenders in Mexico and El Salvador, and pro-democracy activists in Thailand, just to note a few.

There is a report that just came out this month by the digital forensic research lab of the Atlantic Council entitled "Mythical Beasts and Where to Find Them, mapping the global spyware market and its threats to national security and human rights."

They identify companies in India and Italy and Israel as being some of the main sources of selling this spyware to regimes around the world. It also goes on to say that this is a very thriving market, and there are a lot more actors joining this.

I think the one that got early attention, of course, was when NSO technology was used by the Saudis to essentially track and monitor Khashoggi's fiancée at the time, leading ultimately to his death.

The Administration, the Biden administration—I give them credit—they have worked to try to raise the costs to these companies that are engaged in this commercial spyware and selling it to these regimes including by putting them on the Entities List and other measures. You mentioned some of these in your opening statements.

Could you elaborate a little more on your assessment of whether or not those penalties have been effective and then elaborate a little bit more on some of your suggestions on whether you think

there are more things we should be doing right now to raise the costs on those companies?

Mr. KAYE. Mr. Chairman, thank you for that question.

Let me answer in two ways. The first is on raising the cost. I do think this is not only the Biden administration; it has actually been on the basis of law that has been enacted by Congress in the last couple of years where you have had both the normative development against foreign commercial spyware, and you have had the Administration through the Commerce Department and the Treasury Department's OFAC imposing pretty strict restrictions, essentially sanctioning spyware companies from around the world, and the early evidence—and I stress that this is early evidence—but the early evidence is that these costs are actually having an impact on these companies.

We see that in a number of areas. We see that in reporting. We see that in the change that some of the companies are undergoing. So I think there is a movement although, again, it is early.

I think the next step is recognizing that the United States cannot do this alone. This is a global problem, as the reporting by the Citizen Lab and Amnesty and Access Now have indicated. It is a global problem, and it requires a global solution.

Now, the Biden administration has pulled together a number of other states in order to push similar kinds of approaches that we have done at home. I think these other states are somewhat lagging behind. I think a bit of congressional pressure and support for those Biden administration initiatives would be extremely valuable.

I also think that it would be valuable for Congress to look at ensuring that those victims, particularly victims in a transnational repression context—those who are in the United States, because we have evidence of people in the United States being targeted by different forms of either mercenary spyware or other kinds of hacking—that those individuals can actually take action themselves, bring suits against states.

Now, those suits are often barred, often by the Foreign Sovereign Immunities Act, but there may be some room there, I think, for Congress to consider whether there might be a benefit to ensuring that some remedies are available.

So I think there is a lot of room to increase those costs. There is a lot of global space to do that, and I think that, honestly, Congress and the Biden administration have been on the right track. There is a good trajectory there.

Senator VAN HOLLEN. Thank you.

Senator Romney.

Senator ROMNEY. You have each spoken about or not—I think almost everyone has spoken about a free and open internet, and I am not sure entirely what that means.

We would obviously believe that all of our information sources should be available. The Chinese and Russians and others would think all of their information should be available.

There would also be massive disinformation. We are seeing that now. I wonder whether the day is coming when the American public stops looking at the internet for information because it is so overwhelmed with information coming from bots—made up stories, made up pictures.

So when we talk about a free and open internet, I do not know precisely how you determine that. Are we going to—are we going to—if you will censor Russian bots? I guess I think yes, but then it is no longer free and open. And how do you—how do you define a free and open internet?

Because I am sure Xi Jinping would say that is what we have—we have a free and open internet. All the information that people need to see, all the truth as he wants people to see it, is there. And we disagree. We think what they have is false.

But so who determines and how do we assess what is a free and open internet, and do we limit disinformation? Who decides if it is disinformation? This is—I mean, obviously it is something we are struggling with just here at home.

Mr. Kaye, it looks like you have a comment on that.

Mr. KAYE. Thank you for that question, Senator Romney.

It is a very good question, and it is an important question that I think is actually quite complex. At the international level we have basic rights to freedom of opinion and expression, and it is a robust right, actually. The international right is the right to seek, receive, and impart information and ideas of all kinds regardless of frontiers.

So it is a right that should enable us to access information, and when we think about subjects like disinformation and how you restrict that, once we start to go down that path we actually start to give the authoritarians a kind of opening to censor because their view of what is disinformation is not our view of what is disinformation.

So there are a few things that I would sort of point to here that I think are valuable for us to think about. First off, on the normative side—I hate to bring up norms—but the Human Rights Council, the U.N. General Assembly, have very much pushed this idea that international human rights apply online as much as they do offline, and that is part of the normative shift that has happened within the international community.

It is being pushed back against by China, by Russia, and by many others. I think we need to continue to push for the idea that individuals should have access to all kinds of information.

I think we could also promote ideas that would essentially involve both the private sector and public actors in being involved in determining sort of the security that is required for people to engage online.

I think this is a big part of what OTF does.

Senator ROMNEY. I am going to interrupt just because I have to go to another hearing, and I want to just follow up a bit on this avenue of disinformation and open and free internet, what it means.

Right now an entity can publish an absolute lie and slander someone, libel someone, and there is no recourse for that individual because they do not know who did it. They do not know whether it is a bot or a person, and the internet company is free from liability as well—the social media company.

I do not know what the answer is to deal with this disinformation and slander and libel that occurs and wonder should we insist that the social media companies determine that there is

an individual or an entity that is actually posting something on the internet so that there is recourse if someone wants to bring an action against either a government or an institution or a person, as opposed to right now when there is absolutely no awareness whatsoever of who is behind a post and who is responsible for it?

Ms. Cunningham, I will turn to you and Mr. Kaye and Mr. Jaffer. We have not got much time but any thoughts on that?

Ms. CUNNINGHAM. Well, actually——

Senator ROMNEY. All right. All right. OK.

Yes. Mr. Kaye.

Mr. KAYE. Well, I would say that we ought to look to actually to the European regulation, the Digital Services Act, which tries to address this problem in a way that we have not and their fundamental approach is transparency, on the one hand, but also risk assessment, an actual requirement that the companies conduct the kind of risk assessment to prevent the kind of harms that you are describing, and then requiring that there be some mechanisms of appeal for an individual who faces these kinds of harms.

It is a very tricky and narrow path to walk, I think, between demanding transparency and recourse and promoting and protecting rights to free speech.

I think that is exactly where you are suggesting there is a problem, and I think that we should—we could learn something from what the European Union has done in this case in trying to address——

Senator ROMNEY. We are in trouble if we got to learn from the Europeans. But maybe you are right.

[Laughter.]

Senator ROMNEY. Mr. Jaffer, anything you want to say on that regard?

Mr. JAFFER. No, I think that is exactly——

Senator ROMNEY. By the way, I agree. That was humor. I agree.

Mr. JAFFER. I too actually worry that when we look at the European regulatory approaches to the solution to America's problems on free speech, right. I actually think that could actually have significant innovation challenges.

I think at the end of the day what we have got to figure out is how do we protect anonymous speech, which there is a long history of in this country, right, while also addressing disinformation and misinformation, while also ensuring that we are providing capabilities to people who live in unfree societies to talk about the things they want to talk about and get the news from us.

I have to say I think the only solution to this challenging problem you raise, Senator Romney, is recognizing that there is not a moral equivalence between what we do and what the Chinese do.

When the Chinese or the Russians or Iran conduct surveillance, they do it in a one party state with one control. No judges. No independent authorities.

When we conduct surveillance, we have got to go to judges. We have to have review. Congress reviews it. There is a lot of oversight, and ultimately a judge weighs in.

And so, at the end of the day, I think that is the difference. It is not the same when we talk about their disinformation versus ours, or our legitimate information versus theirs.

There is a fundamental distinction, and when we all embrace that fundamental distinction I think at the end of the day, you know, it is fine to put in place rules that require disclosure of names and addresses if somebody is violating American, or in the right case, European law, right, and it is OK to say, no, China, Russia, you cannot get that same thing because you are an authoritarian society.

It is just a different system, and it is OK to say when they do it it is different, and when we do it it is OK.

Senator VAN HOLLEN. Thank you, Senator Romney.

Senator Ricketts.

Senator RICKETTS. Thank you, Mr. Chairman.

All right, Mr. Jaffer, I want to pick up our conversation.

One of the things you said in our first round of questioning was we need to push back harder against Russia, China, Iran.

Talk to me. What are some of the specific steps you think that we need to do to push back harder on these bad actors?

Mr. JAFFER. Well, look, Senator Ricketts, you know, we——

Senator RICKETTS. Specifically talking about cyberspace on this.

Mr. JAFFER. Yes, fair enough.

The same theory actually applies to the real world as well. For all too long in the cyber domain we have accepted that China steals billions of dollars a year, trillions of dollars in total of American intellectual property.

We have accepted that the Iranians and North Koreans both conducted destructive attacks in the United States back in 2015, right—Las Vegas Sands and the Sony Corporation.

We have accepted that, and we have not pushed back. We have not hit their systems. We have not taken other actions in the real world whether—you do not have to respond in cyber, right, with a cyber activity. You can respond in the real world with a cyber attack but we have not responded.

We have taken it on the chin over and over again, and what that does is it creates more risk. It incentivizes bad actors to try and test where our boundaries are.

Now, it is clear that some of them know where some of our boundaries are. We have not seen a major takedown of our energy grid or our banking system even though we know some of the most cable actors—China, Russia—have that capability, right, and we have seen, although it got close with Colonial Pipeline with Russian sort of supported ransomware actors.

So we know there are some bounds that they recognize. The problem is that if we do not hit them back, and we do not do it in a way that is public, that we cannot effectively then deter our adversaries or their friends from coming back against us, and we have just taken our weapons off the table. We do not talk about the red lines and we do not enforce them.

Senator RICKETTS. So when you talk about hitting them back are you talking about we should conduct cyber attacks against them? And I think one of the reasons we do not do that is so we preserve our capabilities so they do not know what we can hit them with.

But are you also talking about, like, sanctions? What are you talking—like, what are the specific things? You say hit them back. How do we hit them back?

Mr. JAFFER. I think all the above. But let us talk about cyber capabilities because I think that is a really good point, and you are exactly right. Too often we say we do not use cyber capabilities because we do not want them to know what weapons we have.

But the same is true in the real world, right? There are a lot of weapons we keep secret, we keep classified, but there is a lot of weapons we talk about that we have and we use, right?

If we are going to effectively deter, you got to talk about where your red lines are. You have got to talk about what you are going to do if those red lines are crossed, you have got to talk about the capabilities you have to enforce those red lines, and then—last piece—when those red lines are crossed you got to enforce them.

We do not do any of that. We do not talk about capabilities. We do not talk about red lines. We do not enforce them, and so it is no surprise that our adversaries are testing our boundaries. They do not know where they are, and they do not know what we are going to do, and then when it happens we do not do anything.

Senator RICKETTS. All right. I want to go back to this other thing too because we talked about Ukraine and Russia attacking them and not being discussed when you said it was with American technology, American companies, helping out.

So why do you believe that our systems are so much more vulnerable than Ukraine from a Chinese attack or a Russian attack, you know, if they wanted to do that?

Mr. JAFFER. I think a couple of reasons. One, we are innovating rapidly here in the United States as we deploy new capabilities. They are not necessarily built with trust, safety, and security in mind at all times. I think that is a key thing.

We have got to incentivize that kind of behavior, and that comes both from investment but also from light touch, you know, regulation. The government can use the way that it spends its money to get companies that sell to the government to build more trust, safety, and security in their systems.

And then, finally, I think that, you know, in the United States it is harder for the public and private sectors to partner, right. There is a lot more challenges to it.

Private industry is afraid of regulation. They are afraid of lawsuits. The government itself is afraid of giving classified information to the private sector, right, and giving it at scale to the private sector.

We have talked about it for decades. We have not done it effectively. Those problems were a lot less true in other countries, including Ukraine, where the public and private sectors work a lot more closely together.

Senator RICKETTS. OK.

And again, I am kind of running out of time here but can you just talk about what are some of the most critical steps that the U.S. needs to do? And I am looking for specific things we can do to be able to enhance our cyber capabilities to successfully be able to deter the PRC?

Mr. JAFFER. Well, I think, one, we have got to spend a lot more on the cyber capabilities. We are underfunding our Defense Department across the board including in the cyber domain.

We have got to give them the best cutting edge capabilities. We have got to get them to lean forward. They also, for their part, have to be willing to buy and build with the private sector effectively.

All too often the government says we have got to build it ourselves internally, or we are going to buy from the five defense contractors we always buy from.

We have got to break that mold when it comes to emerging technology. We are not going to be able to do this without cutting edge startups.

And as for investment starts today, I can tell you it is very hard for a startup. You know this, having done this in Nebraska. It is very hard to start to sell to the government. It is a no win. They want to do it. They cannot do it.

And at the end of the day, I think that if we continue to over regulate, if we take the European model—Digital Services Act, Digital Markets Act, GDPR, right—which a lot of people think we are behind the Europeans. We are actually ahead of the Europeans.

If we adopt European regulations, all that will do is harm the ability of the U.S. to innovate and take our best players off the field. That is a terrible idea.

The reason why Europeans do not have great innovation, they over regulate it right at the jump. We should not make that mistake, particularly not in the AI domain.

Senator RICKETTS. Great. Thank you very much, Mr. Jaffer.

Mr. JAFFER. Thank you, Senator.

Senator RICKETTS. Mr. Chairman.

Senator VAN HOLLEN. Thank you, Senator Ricketts.

So I just want to follow up on some of these particular issues.

First of all, thank you, Mr. Jaffer, for mentioning the issue of protecting American IP. Years ago I authored a bill called Protecting American Intellectual Property Act along with former Senator Sasse, which is trying to get away from the fact that companies' only recourse sometimes is to go to court in the United States against foreign actors, where even if you get a good decision it is hard to actually enforce.

The idea is to give the U.S. Government more tools where you have a pattern of theft of intellectual property of strategic value that we can go after and sanction them. We need to use that tool more effectively.

I do just want to say with respect to international norms I agree with you, Mr. Kaye, they are important. I do not think anyone is under an illusion that we are going to convert China to our way of thinking, or Iran.

But what we can do is try to both raise the costs and increase the benefits to countries and the rest of the world to follow the norms of an open internet or not engage in selling of commercial spyware or whatever it may be, and that has value if we are talking about sort of digital authoritarianism and our efforts to combat it.

We have got to create these rules of the road, try our best to do that, and then work very hard to try to enforce them through both carrots and sticks around the world. So I think that is what we are really focused on here.

Before I leave the issue of commercial spyware, I do want to ask you about that because I think you referred to it. But the Biden administration through a White House statement did try to get a bunch of countries—and I think they got 17 countries—to sign on to a resolution, a document about adherence to rules about not allowing companies in their countries or discouraging companies from exporting commercial spyware to authoritarian states.

Am I right about that?

Mr. KAYE. Yes. I think actually as of 2 days ago there are 21 states that have—that are part of this including the United States, and the objective is not only to promote stricter export controls so that spyware is not allowed to proliferate the way it has but also to ensure that there are conditions on relationships and on the sale of technology to states that are committed, and not just committed in a sort of paper thin sort of way, but in an implementable sort of way that they are committed to observing human rights in the use of the technology.

So that effort, I think, is part of what I was suggesting before is that the United States can do a lot on its own, but most of this really does have to be multilateralized in this particular field.

Senator VAN HOLLEN. Well, I do not know which additional countries just signed on, but I do know that the three I countries, as they say—India, Italy, and Israel—that were identified in this Atlantic Council report were not part of the original 17. Are they part of the 21?

Mr. KAYE. I do not believe that any of those three are. I would have to check the list.

But you are right. When you look at the list, it is actually a very interesting list, and maybe one I could just identify to give a good example of both the threat and the response to it.

So Poland has joined this effort, and of course, there has been a change of government in Poland. The previous government engaged in pretty massive spying on journalists and opposition figures within Poland, and the new government—the newly elected government from last year—has begun to sort of peel back what actually was taking place, and they found that there were literally hundreds of individuals who were targeted with Pegasus spyware, and they have taken the decision that there needs to be accountability for that use.

In a sense, they are modeling something that the United States is encouraging, and in a way they are modeling it to other states. They are not modeling it just to us because, as Jamil said, we have the rule of law in the United States, and we need others to demonstrate that they have it, too.

So I think there is—you know, it is really not just a question of having states sign up to this statement on its own, but it is having them sign up and do the things like Poland is doing to actually demonstrate that they mean business and they mean accountability.

Senator VAN HOLLEN. And what would you suggest the United States do for countries that choose not to participate in this? We talked about some of the things we can do with respect to companies by putting them on the Entities Lists or, you know, visa sanc-

tions on individuals who work for companies. But how about at the country to country level?

Mr. KAYE. On the export side, I think there is quite a bit that the United States can do to encourage compliance.

It is difficult in part because, as you noted earlier, the spyware industry is a massive industry that is incredibly remunerative and economically beneficial to the countries where they are headquartered.

So we are fighting against that. But I do think there are kinds of conditions that the United States can impose. I do not mean conditions on our entire relationships with countries, but conditions on certain kinds of support and cooperation that are related to the end user.

In other words, the client country's use of technology should be based on fundamental human rights norms, and we can do some conditioning in terms of what we share, what our relationship looks like in order to move them.

We have that power to move them in a positive direction. I think some of that if it is embedded in law as well could be also extremely valuable.

Senator VAN HOLLEN. Thank you for that.

I want to turn briefly to the tools for mass surveillance which we see in use in China, and China, of course, also making available for export to other countries that want to adopt a lot of these tools.

Now, obviously, facial recognition has some beneficial uses that can be used with proper guardrails and rules with respect to law enforcement, but the line gets very murky, as you all know.

My colleague, Senator Merkley, has been very focused on this. Now when you go through TSA you get your picture taken, although you can opt out. But we are trying at least to—whether we can have a debate over what rules should apply, but obviously that debate is not happening in places like China or elsewhere where these technologies are being applied.

The Bureau of Industry and Security at the U.S. Department of Commerce recently published a proposed rulemaking that creates a control for facial recognition.

Could you talk about how this technology is developing very rapidly and what your thoughts are and what kind of guardrails we can put around those and again, try to create global norms?

And after Mr. Kaye if any of you others want to answer that question please feel free to jump in.

Mr. KAYE. Sure. Thank you, Mr. Chairman, for that question.

I will answer briefly. First, I would say that we need to be thinking about what kind of society we want to live in and what we want to construct, and we, I think, just have to recognize that some of these technologies are already in vast, nefarious, authoritarian use in places like China, and we see that, for example, with respect to the Uyghur population in the west of China.

The surveillance state that you have there is, clearly, not the kind of state that we as Americans deserve to live in. And so I think that perhaps as a first order of business we need privacy protection. We need nationally enforceable privacy law in the United States.

We also need continuing strong commitment to fundamental digital security tools, in my view, including encryption technologies. These are the kinds of technologies that can protect us. But also I do not think that we want to put all of the onus for protection on the individual herself.

The protections need to be legal protections, so my view is when we are talking about things like facial recognition, affect recognition—all of these tools that essentially interfere with our ability to be anonymous when we are out in the world—I think we need to be thinking about legal protections like a national privacy law.

Senator VAN HOLLEN. I appreciate it.

Do either of the other two—if you want to comment on that question.

Mr. JAFFER. Senator Van Hollen, I think privacy laws are interesting but GDPR in Europe has not stopped mass surveillance, right. Encryption technology is important. Has not stopped mass surveillance in the United States or anywhere in the globe.

So I think the real way to do this is the reason why these things are so lucrative is because people will buy them, and the reason why they can build them is because people will invest in them.

If we can starve them of capital, that is one way to solve this problem. Now, not all surveillance tools are built alike, right. There are surveillance tools that are used by democratic societies that are appropriate use under the rule of law, right.

Our group of investors—our trusted capital group investors, 19 investors around the globe including in Poland, has come together and committed to not selling or building technologies that will be used by our adversaries.

We have committed to only building technology capabilities that are used by America and its allies. Now, of course, right, that is because we believe in free and open societies.

It is OK for the U.S. Government and other governments that have the rule of law to use surveillance technologies in appropriate ways. So there is no upside to saying we are not going to invest in those, but we are not going to invest in capabilities nor invest in companies that sell to these adversary nations.

And so if you have investors making those kind of commitments and saying, we are going to bake trust, safety, and security into our tools, we are going to follow the NIST framework, we are going to follow these AI frameworks and the like, and we are not going to invest in adversary technology, that is the way to starve some of these companies who build these technologies of capital.

Now, other capital providers will, of course, step in—China, Russia, Iran. Sovereign wealth funds may step in. But then the government can take action against those.

So there is an appropriate space for the government to act. There is an appropriate space for private capital to act, and the question then just becomes can we convince other private capital actors to get in this and to ultimately build and buy technology that is actually protected, secure, and capable.

Senator VAN HOLLEN. Thank you.

Starting with you, I think, Mr. Kaye, on this legal question. But again, if the other witnesses want to answer it please feel free to do so.

Last month the U.N. ad hoc committee on cybercrime adopted the U.N. Convention Against Cybercrime, setting up a critical vote in the U.N. General Assembly I believe later this year.

I think we can all recognize that there would be benefits of having a common understanding across nations for what is considered cybercrime. But critics of the draft text have raised concerns about this treaty, that it would put at risk privacy and data and the safety of dissidents, journalists, and activists around the world. I believe that it was Russia that first put forward this draft.

I believe the United States and others have pushed back against certain provisions, and changes have been made, but the question is whether the changes that have been made are adequate to address the concerns about privacy and continuing to expose dissidents around the world to unfair use of the terms of the draft treaty.

So, first of all, as the Biden administration considers its ultimate position on the treaty could you clarify for the committee what issues the current draft presents as it relates to potentially being used and abused by autocratic countries to legitimize digital repression?

Mr. KAYE. Thank you, Mr. Chairman, for that question.

So you are absolutely correct. I mean, this was a Russian initiative originally to put forward a global cybercrime convention.

Of course, there already is a cybercrime convention, the Budapest Convention on Cybercrime, and at a strategic level I would say that because the Budapest Convention, which admittedly has some of its own sets of problems, has stronger protections for human rights, also for states that want to resist abusive uses of cross-border legal procedures, that we should be encouraging states to join the Budapest Convention, not to join this new U.N. cybercrime convention.

And I think the proof of the problems to a certain extent in the cybercrime convention is the array of industry, of companies, of civil society that have expressed really grave concerns and actually have expressed grave concerns about this convention as it was being negotiated for the past several years.

I would just give one little example, and the example is how the convention defines " serious crimes" according to how severe the penalty would be for that.

But if a matter is identified as a serious crime, it provides a state with the ability to request data, including personal data, subscriber data, and others across borders, and I think that is something that puts in the hands of authoritarians, including governments like Russia, the ability to seek information and to weaponize their law in a transnational sense that is just deeply, deeply problematic.

And certainly it is problematic at this particular moment when, as the subject of this hearing indicates, there is a very serious rise of authoritarianism in cyberspace.

So my view is that at the very least the United States should abstain when this comes to a vote. But more generally, strategically, we should be encouraging states to join the Budapest Convention.

Senator VAN HOLLEN. Thank you.

Do either of the other witnesses want to comment on this?

Ms. Cunningham.

Ms. CUNNINGHAM. I think to Ranking Member Romney's point about kind of norms versus technology, this goes back to that for me in that I think it is critical that we are investing in both of these areas.

Certainly, it is the case that we are not going to get China and Iran and Russia to start implementing a democratic internet. But my bigger concern from a technical perspective is that they are actively promoting their norms around the world. The Cybercrime Convention is a great example of that, but we see it from a technical perspective as well.

China, Iran, and Russia are engaging in technical standard setting bodies as well to try and fundamentally even redefine what the internet looks like from the inside out, trying to undermine interoperability, trying to undermine security.

It becomes even more critical that we are thinking about norms from a legal and policy perspective, but also a technical perspective when we know these other governments are investing time, money, and energy in terms of trying to redefine what the internet looks like itself.

Senator VAN HOLLEN. Thank you.

Mr. JAFFER. Senator Van Hollen, I agree completely with what Mr. Kaye and Ms. Cunningham have said on this topic. I think the idea that the U.S. spent the better part of 3, 4 years actually creating a separate process to develop this treaty, have an existing convention that we are part of, and then now it sort of changes its position is odd, and I am hopeful that when it comes to the General Assembly here in the next few days or next few weeks that there will be a different outcome.

I mean, I think Ms. Cunningham's point is an excellent one which is, you know, the role that these unfree countries—China in particular, but Russia, Iran, North Korea as well—are playing in some of these bodies, whether it is the U.N. Human Rights Council, or you know, ITC or the like, there are a lot of organizations that are setting standards and rules in key areas of technology where they are able to get the jump on us and then embed the kind of tools—the kind of rules that would then empower Chinese technology to get in, I think that is very problematic.

That is why it is so critical that the U.S. Government is already on this issue. They are putting a lot more of our people in these spots. But it is also important to bring American industry in as well.

American industry is so critical to these standard setting bodies that it has got to be a partnership between the government and industry. Simply putting more government people in these seats is part of the answer, but it is not the only answer.

Senator VAN HOLLEN. Thank you. So it is your view that if the United States had to vote today on this treaty up or down that you would at least abstain. Am I understanding your answer correctly?

Mr. JAFFER. I would vote against it.

Senator VAN HOLLEN. So we are coming toward the end of the hearing, but I do want to just give each of you a chance to cover any issues that you think that we have overlooked both in terms of the issue itself but most importantly recommendations that you can make to us as a Congress.

Obviously, the Administration can use the tools available through executive action.

Mr. Kaye, you have already identified some additional legal changes that we might consider here. But I just want to give you all that opportunity.

I do also—if you could—this issue of standard setting bodies, international bodies, is really important because it is part of the conversation about the normative battle.

I mean, it is not disconnected from that. It is directly connected to that, because that is actually where the rules get put into place that govern the international use of these technologies.

So maybe as you answer this question you could also just point out where you think at this particular moment we need to be doing more with respect to those international standard setting bodies.

As you said, Mr. Jaffer, the Administration has increased its focus on this, trying to deploy more people there, but this is an ongoing battleground.

So this is just an invitation, really, to make whatever sort of closing remarks you want to make, Ms. Cunningham, and then we will just go down the line.

Ms. CUNNINGHAM. I will start by saying, I think we have debated a lot about technology and norms today and I think it is critical that we do both. I think to try and choose one of the two would ultimately mean that we fail in this endeavor.

I think when it comes to staunch authoritarians like China, Iran, and Russia we need to find ways to raise the cost by investing in novel technologies that can help protect human rights, and also provide anti-censorship and security capabilities to citizens domestically so that they can push back on authoritarianism where it is starting.

I think we also really do need to focus on norms, because the reality is that Russia and China are exporting these technologies, and not just the technologies—the training and the beliefs that come with them, to over a hundred countries around the world.

And even if norms may not win the day in China and Iran, there are many countries across the Belt and Road in Africa and Latin America that we still have a significant potential to influence. I think if we are to lose focus on them we will lose the larger battle in terms of defining what a democratic internet could really look like.

To your question about standard setting bodies, one of my concerns with this issue is that it is often seen very narrowly in a human rights perspective when, frankly, it has huge implications, as we have talked about today, for national security, for our democratic principles.

And so when we think about where we need to engage on this issue in standard setting bodies, the first thing that I would encourage us to do is look across the board at all the places where cyberspace is being raised and make sure that we are engaging on this issue not just from a human rights perspective, which is critical, but from all of our national security and foreign policy interests.

One place that we engage particularly that I think could use more focus is the IETF, but there are a number of different places

where China and Russia are raising these issues, and we are underrepresented.

Senator VAN HOLLEN. Thank you.

Mr. Kaye.

Mr. KAYE. Thank you, Mr. Chairman.

I actually share everything that Laura just said and would only add a couple of additional points.

The first is on her point that I think we have been all talking about, a situation where human rights and national security actually align.

In other words, our interests in a robust human rights approach to new technologies, to intrusive technologies, is very much also a question of U.S. national security, and we can point to example after example, I think, as we have all indicated of where there is an alignment there—that the human rights abuse is also a national security threat.

And so if we think in those terms I think there is a way to think about how we engage in different international forums and why we do and what we invest in.

So to give just one example of a forum that I think is extremely underresourced, also occasionally under serious criticism, is the U.N. Human Rights Council where the battles there are sometimes normative but sometimes they also lead to change in law at domestic levels.

And I think that is a space where the United States as it has actually over the last few years has increased its voice there could continue to do so. Also in the ITU there is room to do that kind of work where, you know, the head of the ITU is somebody who is well known in Washington.

I think there is a lot of room to do that kind of work in those settings including the other standard setting bodies that were mentioned before.

But I think that is the place that I would tend to focus on. I think that, as we have discussed, all of those come together as a question of both national security and fundamental human rights.

Senator VAN HOLLEN. Thank you.

Mr. JAFFER. Thank you, Senator Van Hollen.

The only thing I wanted to mention was we spent a lot of time today talking about a lot of the challenges that technology can pose to free and open societies, to Americans here at home, to repressed peoples abroad.

I want to focus on the fact that technology has actually benefited the globe tremendously. American technology has benefited free and open societies around the world.

It has raised standards of living around the globe. It has provided opportunities for people in free and unfree societies to have access to information in ways that have been transformative.

I feel the same way about AI. AI has its challenges, to be sure. It can empower authoritarians and the like. But writ large I think artificial intelligence and the broad adoption of it will actually be a tide that raises all boats, that creates opportunities, creates new jobs, creates innovation, and creates economic benefits not just here in the United States and in our allied countries, but around the globe.

And so I am actually very heartened by the transformative power of technology and the transformative power of systems like ours that allocate capital toward innovative capabilities and that drive us toward freedom and democracy.

And so while we have our challenges in this country, and there are plenty, and our system is not perfect it is the best the world has ever seen, and it is one both in the form of allocation of capital, economic liberty, but also in freedom of speech, freedom of thought and the like, and it is an idea that we have got to once again embrace.

All too often we focus in on the threats of the challenges we face, and there are tremendous ones both in this country and abroad, but we also need to embrace the fact, I think, as Americans and as folks in societies that are free and open that we have responsibility to give that capability and that opportunity to others around the world.

That is why the work that OTF is doing is so critically important. That is why setting these norms is important but it is about once you set the norms enforce them in living by them, which all too often we talk about them, and they become aspirational and do not become practical.

At the end of the day, I think that the opportunity that you have given us to talk about these issues, the work that you and the ranking member are doing on these issues to [unintelligible] them here in the Senate and that folks in the House are doing as well is so critical.

And thank you for the opportunity to be here, and thank you for your attention to these important matters.

Senator VAN HOLLEN. Well, thank you all, and you are absolutely right. I mean, these new technologies have huge potential benefits.

I mean, technologies are not in and of themselves good or bad. They can be put to good purposes. They can be put to bad purposes, and I think one of the things we want to do in this hearing, as you have all expressed, is maximize the good and the benefits and minimize the harm and that is not easily done. It requires, I think, thoughtful conversation.

So thank all of you for being part of it. It has been a very engaging discussion. Thank you.

And with that, the record will be open until close of business of Wednesday, September 25th, and again, thanking all of our witnesses.

The hearing is adjourned.

[Whereupon, at 11:39 a.m., the hearing was adjourned.]

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

RESPONSES OF MS. LAURA CUNNINGHAM TO QUESTIONS SUBMITTED BY SENATOR BRIAN SCHATZ

Question. U.S. technology companies actively comply with the People's Republic of China system of digital authoritarianism in order to operate in the country, including by removing VPNs and other democracy-promoting applications from app stores at the behest of the PRC. What can we do to raise the cost of this compliance, including by making it more public?

Answer. The U.S. private technology sector is often excluded from important markets unless they are willing to make unreasonable accommodations to authoritarian demands—a choice between their bottom line and respect for democratic values and human rights. This tension is evident with respect to app censorship, wherein thousands of apps, including many internet freedom tools, have been removed from app stores at the request of the Chinese government as a form of meta-censorship.

To place the scale of China's app censorship in perspective, a report from OTF partner GreatFire's App Censorship project found that 66 of the 108 (61 percent) most downloaded apps worldwide were unavailable to Chinese iOS users, compared to only 8 that were unavailable in the U.S. Apps categorized as news, books, and social networking are disproportionately unavailable in China. Notably, Apple's own News app has been removed. So-called "sensitive categories," which include many OTF-supported technologies like VPNs, privacy, and digital security, along with religion (especially related to apps for Uyghur or Tibetan users), are also disproportionately censored. In the lead-up to the commemoration of Tiananmen Square in 2022, for instance, the secure messaging app Session was removed.

App censorship as a form of information control is not limited to the PRC, and instead is being adopted by other digital authoritarians as further evidence of autocratic learning. Another report from GreatFire's App Censorship project found that Apple removed over 50 VPNs from the Russia App Store this summer, double the number reported by Roskomnadzor. The discrepancy suggests the scale of VPN app removals is much larger than publicly acknowledged, and that Apple may be proactively removing more VPNs than authorities have expressly requested.

OTF continues to make investments in censorship monitoring platforms to enhance transparency. However, increased public disclosure requirements related to app censorship and the precise nature of how governments mandate removals would be beneficial. Companies are currently required to disclose cybersecurity incidents to the U.S. government; they could be required to do the same when they enable censorship and surveillance by autocratic regimes or by states that are designated as foreign adversaries. While Apple reports on the total number of apps removed worldwide because of a government takedown request, this information is not disaggregated or specific. It also does not include which apps are later removed globally, or for vague violations of community standards. A wider range of public reporting would provide policymakers with missing information to fully understand the breadth and depth of authoritarian app censorship.

Question. How much demand for Virtual Private Network (VPN) technology does OTF estimate there is amongst global civil society organizations, what amount of that is OTF able to fulfill, and how much additional funding does OTF estimate would be needed to cover the difference?

Answer. Today, two-thirds of the world's population—nearly 5.5 billion people—live in a country where the internet is censored. In the last 2 years there has been a marked acceleration in the speed, scale, and efficiency of digital authoritarianism, such that OTF has seen a more than 500 percent increase in demand for the VPNs we support. We regularly supported about 9 million VPN users each month for over a decade, but as a result of bipartisan support from Congress and a one-time allocation from the State Department, we are now supporting over 45 million users each month.

And demand continues to grow globally, including in Iran and Russia, but also in Belarus, Cuba, Ethiopia, Myanmar, Syria, Venezuela, and more. This growth indicates that VPNs are no longer solely for the most at-risk populations: they are an essential prerequisite for billions of people around the world who want to access the global internet as we experience it.

However, the surge in demand for secure, trusted VPNs is quickly outpacing the public resources that are available. In order to stretch Federal funding, we have worked with VPN providers to reduce their costs as much as possible to less than one dollar per year per user. Similarly, we have engaged the private sector on ways they can further contribute.

Despite these cost-saving efforts, OTF is anticipating a $10 million budget shortfall for VPN support in fiscal year 2025. As a result, we will be forced to cut off as many as 14 million monthly users in priority countries. In addition, we anticipate demand for OTF-supported VPNs to increase 150 percent by fiscal year 2027 to approximately 70 million users per month.

Question. What is OTF doing to strengthen the ability of civil society organizations around the world to coordinate amongst themselves and defeat digital authoritarian technology? How can Congress further support this crucial cooperation?

Answer. Once only available to a small number of well-resourced autocrats, highly advanced surveillance technologies are now widely accessible to nation-states and other illiberal non-state actors around the globe. Over the last 10 years at least 75 countries—nearly 40 percent of all nations—have acquired commercial spyware, giving rise to a mercenary spyware industry now worth an estimated $12 billion per year.

This pervasive use of accessible and affordable spyware and digital surveillance technologies by authoritarian regimes has made civil society organizations more vulnerable than ever. In many countries, civil society organizations are working individually in isolation to identify and mitigate digital threats to their organizations and communities. While some groups have stepped forward to investigate and analyze new surveillance tools and techniques, they remain few in number, underresourced, and cannot respond quickly to the immense volume of new threats spread across different regions. The lack of coordination often means that organizations spend too much time and money on digital threats, and still often miss important critical vulnerabilities. Even known actors in this space like Citizen Lab agree that there is an urgent need for coordination among civil society organizations to collect, analyze, and ultimately mitigate digital threats and attacks.

To this end, OTF is supporting digital "helpdesks" to increase threat intelligence expertise and coordination among local and regional civil society organizations in order to effectively combat authoritarians' enhanced and coordinated surveillance efforts. For example, OTF supported the Tibetan Computer Emergency Readiness Team (TibCERT), a formal, coordinated structure to identify, analyze, and mitigate online threats to the Tibetan community—a frequent target. In addition to significantly improving the digital security of the Tibetan community, TibCERT has played an invaluable role in quickly identifying and exposing new technologies and tactics being deployed by the Chinese government globally.

This example is illustrative of a larger model that can be scaled and replicated in other contexts. Our investments in digital security consistently show us that increasing threat intelligence expertise and coordination among local and regional civil society organizations can effectively combat authoritarians' enhanced surveillance efforts. An additional $10 million annually would allow for the establishment of a global civil society threat intelligence coordination network to fill existing forensic research and coordination gaps. These funds could support at least 10 local/regional digital security helpdesks to quickly identity and respond to novel digital threats; local researchers to conduct in-depth forensic analyses of identified threats and tactics; and regional and global coordination networks to rapidly alert journalists, human rights defenders, and civil society organizations of identified digital threats and share effective mitigation strategies.

RESPONSE OF MR. DAVID KAYE TO A QUESTION
SUBMITTED BY SENATOR BRIAN SCHATZ

Question. How are authoritarian states like Russia and China using international bodies like the U.N. to advance digital authoritarianism? What further should the U.S. Government, specifically Congress, be doing to counter this?

Answer. Russia, China and other authoritarian governments advance their interests within the United Nations system in different, if mutually reinforcing, ways. As I noted in my testimony, China and Russia take very seriously the normative system embodied by the U.N. (even as they do not abide by its rules in their own laws and policies). They tend to play a long game; whereas many authoritarian governments simply seek to avoid censure within U.N. human rights mechanisms, China and Russia see a long-term process which would, if successful, reinforce their national efforts to promote state control, extend the long arm of censorship, and counter democratic states' efforts to maintain and reinforce a free and open internet.

For China, this has involved, among other things, robust engagement with the negotiation of the UN's Global Digital Compact (GDC), in which it has repeatedly sought to include language that emphasizes "cyber sovereignty," that is, a model of internet governance that privileges state control over human rights. It played an active role in the GDC negotiation, courting the main U.N. official guiding the negotiation, the Secretary General's Technology Envoy, and coordinating the approach of the G77 Group within the U.N. It follows a similarly engaged approach across the range of U.N. activity, including with respect to resolutions in the General Assembly and Human Rights Council. Moreover, its efforts go beyond language in U.N. resolutions. In the International Telecommunications Union's World Telecommunications Standardization Assembly, for one example, China has sought to promote an internet protocol favorable to its own economic and political interests and inconsistent

with an internet that enables the protection of digital rights such as privacy and freedom of expression and association.

Russia typically has taken a more aggressive rhetorical and diplomatic approach, even as it shares China's long-term normative agenda within the U.N. system. During my time as U.N. Special Rapporteur on freedom of opinion and expression, Russian diplomats within the Human Rights Council would publicly dispute my argument that individuals enjoy free speech and privacy rights online just as they do offline, going so far as to pretend that freedom of expression did not apply online at all. They echoed this aggressive approach in other forums, such as the Organization of Security and Cooperation in Europe (OSCE), regularly seeking to undermine the OSCE's Representative on Freedom of the Media. Perhaps the most notable recent Russian effort has been its initiation and promotion of the Cybercrime Convention, which the U.N. General Assembly may adopt later this fall. As I suggested in my testimony, the Convention would open the door to a global legal landscape friendly to state efforts to obtain private data of dissenters, dissidents, and journalists across borders. Russia fought hard against even the weak human rights safeguards included in the final text of the Convention draft, but it is on the cusp of getting U.N. approval of a vehicle for authoritarians to seek the information of those it alleges are responsible for the vague category of "serious crimes."

The United States plays a leading role in the global effort to counter digital authoritarianism within the U.N. system and other international bodies. Notwithstanding the example of the Cybercrime Convention, the Biden Administration has been a strong supporter of global digital rights. It has actively supported civil society participation in those spaces where digital rights are considered and negotiated. In order to promote and deepen that role for the United States, I would suggest at least three concrete items for a congressional agenda:

• First, Congress should closely scrutinize the Cybercrime Convention even if a future administration does not transmit it to the Senate for approval of ratification. Such scrutiny, including briefings and hearings with civil society participants in the negotiations, would provide strong insights into how the Convention came to be, what it suggests about authoritarian government strategies to undermine online freedoms, what protections in law should be considered in the face of the Convention's future entry into force, and what support the United States might give to those states likely to face pressure from authoritarian governments to share private data.

• Second, the United States has strong allies promoting digital rights within the U.N. Office of the High Commissioner for Human Rights (OHCHR). A U.S. voluntary contribution to support OHCHR's digital rights efforts would reinforce a chronically under-resourced institution that does work that supports a human rights approach to issues of internet governance. I would urge the Congress to provide substantial funding for this purpose.

• Third, authoritarian governments, as with all governments, including the United States, regularly appear before the Human Rights Council in the context of the Universal Periodic Review (UPR). The UPR is a high-profile moment for many governments to showcase what they perceive as their human rights successes—and for others, including civil society organizations, to point out a country's failings. The United States should make it a standard procedure that its delegates to the UPR highlight the specific policies, laws and practices that authoritarian governments deploy to interfere with human rights online. Congress could play an important role, through hearings and legislative language, in ensuring that U.S. participation in the UPR focuses attention on the authoritarian agenda within the U.N.