CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Statement before the

Senate Judiciary Committee

Subcommittee on Crime and Terrorism

“Ensuring Data Security Against Lawful and Unlawful Threats in the Digital Age”

A Testimony by:

William A. Carter

Deputy Director and Fellow, Technology Policy Program (CSIS)

November 5, 2019

226 Dirksen Senate Office Building

Introduction and Main Points

Chairman Hawley, Ranking Member Whitehouse, thank you for the opportunity to participate in today's hearing on this important topic. Threats to personal data and critical infrastructure remain one of the most important risks facing our nation. Our reliance on digital infrastructure and services has made us vulnerable to attacks by nation-state adversaries and their proxies, and a largely consequence-free environment for malicious cyber activity has given rise to a bustling cybercrime ecosystem trading on the private data of American consumers and businesses. At the same time, the lack of American leadership on key issues like data governance and digital law enforcement has led to the proliferation of counterproductive policies around the world as foreign governments seek to exercise their sovereignty over technology and data.

The cyber domain continues to evolve around us. In the last 50 years, the price of computing power and data storage has dropped by 6-8 orders of magnitude,[1] and the amount of digital data has grown proportionally. The exponential growth of the attack surface as more of our lives move online and connected devices proliferate (the so-called Internet of things (IoT)) has created new vulnerabilities that can be exploited by malicious actors.

The threat landscape is also evolving. Offensive cyber capabilities have become a must-have in the arsenals of even the smallest national governments. The development of a complex and mature criminal economy online has transformed cybercrime, increasing the sophistication of major criminal groups and making it easy and cheap for unsophisticated small-time cyber criminals to commit fraud and extortion at scale. And repressive governments increasingly leverage technology and data to conduct surveillance, marginalize and exclude groups, and crush dissent and control information.

Norms of state behavior in cyberspace have been adopted in a wide range of international forums, including the United Nations, but the lack of a common lexicon and agreed interpretations of international law have hampered compliance and enforcement. Despite years of investment in tools and expertise, law enforcement's capacity to investigate and prosecute cybercrimes remains limited, and cybercrime is largely consequence-free. And while the NIST Framework and international standards for cybersecurity have helped to spread basic awareness of and promote investment in cybersecurity, particularly for critical infrastructure operators, a lack of clear incentives has left significant gaps in our national cyber readiness that can be exploited by a wide range of malicious actors.

Finally, around the world, the lack of US Government (USG) leadership on key issues of data governance has led to the proliferation of counterproductive policies that harm US businesses and create new risks to private data. The status quo is unsustainable for many governments, and a result they are implementing policies like data localization, data retention mandates, and restrictions on encryption that harm innovation and competition and expose sensitive data to abuse. The USG must take steps to enable appropriate and lawful access to data for governments

[1] Lucas Mearian, "CW@50: Data storage goes from $1M to 2 cents per gigabyte (+video)," Computerworld, March 23, 2017, https://www.computerworld.com/article/3182207/cw50-data-storage-goes-from-1m-to-2-cents-per-gigabyte.html.

around the world to push back on the rising tide of counterproductive policies to preserve that access in ways that are invasive, unaccountable, and harmful to innovation and competition.

Filling these gaps in our cyber defenses and establishing effective data governance regimes requires a coordinated approach between the US government, critical infrastructure operators and private companies, and our international partners. The diverse array of threats we face require different strategies to manage them. The goal of my testimony is to amplify some of these issues and to propose potential solutions for how we can implement an effective strategy to deal with this challenge.

Risks to Companies that Collect Data

Collecting and utilizing data has become a key element of modern business. In virtually every industry, data has become a key enabler of efficiency and competitiveness, allowing companies to get better tailored products and services to customers faster and cheaper than ever before. But the data-driven global economy has also brought new risks to both consumers and businesses. These risks can be divided into three broad categories:

1. cyber theft of sensitive data by malicious actors;
2. lawful exploitation of data by governments;
3. regulatory and policy risks to innovation, competitiveness and economic growth.

A coordinated policy approach is needed to address these risks and establish a global governance regime for cyberspace that is sustainable, adaptable, and resilient.

Cyber Threats to Sensitive Data

Cyber threats remain a critical risk to companies that collect and utilize data. Despite significant progress on cybersecurity policy over the last decade, the threat of malicious cyber activity has grown significantly. Malicious cyber actors fall into two main groups, nation states and their proxies, and cybercriminals. While ideological hackers, so-called “hacktivists,” were once a major threat, most sophisticated hackers have abandoned hacktivism due to the draw of the legitimate “white hat” hacking industry or the criminal “black hat” ecosystem. With high-profile takedowns of leading hacktivist groups like Lulzsec and so much money to be made (legally or not) by those with elite hacking skills, launching ideological attacks that risk highly profitable legal and illegal businesses is no longer worth it. Hacktivism has not entirely gone away, but is a far less serious threat relative to criminals and nation-states than it was a decade ago.

Nation states and their proxies represent the leading cyber threats to US networks, with the resources and determination to penetrate even highly secure networks and launch attacks that represent a significant threat to the security of the United States. These adversaries are known as Advanced Persistent Threats (APTs) because of their advanced technical capabilities and their willingness to persistently probe the defenses of hard targets to find vulnerabilities.

While as recently as five years ago we could talk about the “seven sisters” in cyberspace – the seven nations with meaningful offensive cyber capabilities, the US, Russia, China, Iran, North Korea, Israel and the UK – that list has grown rapidly in recent years. The US intelligence community’s 2018 Worldwide Threat Assessment identified more than 30 countries with significant “cyber attack capabilities,”[2] and dozens more are developing or buying offensive cyber tools and services. While not every country is capable of building up significant cyber forces on its own, the growth of the so-called “grey market” for offensive cyber capabilities is an increasingly worrisome trend that has fueled the proliferation of nation-state cyber attacks around the world. Private companies operating legally sell advanced cyber attack tools and services to governments, which are often used in illegal and unethical attacks. For example, NSO Group, an Israeli spyware company, was recently revealed to be responsible for a campaign of attacks on human rights defenders that exploited a vulnerability in WhatsApp.[3]

Nation-state hackers and proxy groups launch cyber attacks to gather intelligence, gain economic advantage, or coerce and threaten their adversaries. For example, Chinese government hackers have engaged in a prolonged campaign in recent years to build a massive database on American citizens for intelligence and counter-intelligence purposes. By exfiltrating data from the USG Office of Personnel Management (OPM), health insurers (e.g. Anthem), airlines (e.g. United) and hotel chains (e.g. Marriott), among others, China’s intelligence services have access to an incredibly rich database on the behavior, preferences, and vulnerabilities of hundreds of millions of Americans. They also gain a detailed understanding of their relationships to USG employees with access to sensitive and classified information.[4] This has significant implications for US national security. Chinese agents could threaten to expose an illicit affair or pay for the medical treatment of a family member of a USG employee in exchange for sensitive intelligence, or use the travel and financial habits of American citizens to identify American intelligence officers.

Another critical issue for US companies is theft of intellectual property and confidential business information. Malicious actors have stolen everything from the plans of the F-35 fifth-generation fighter jet[5] to the confidential terms of bids for infrastructure deals, allowing foreign companies to copy American technology or undercut bids by US companies. These thefts can be a devastating blow to American companies. For example, the theft of IP from US company American Semiconductor by China-based Sinovel nearly destroyed the company.[6] And nation-states utilize a wide range of attacks to steal US companies’ sensitive data beyond just cyber

[2] Daniel R. Coats, *Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2018), 5. https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

[3] Will Cathcart, “Why WhatsApp is pushing back on NSO Group hacking,” *Washington Post,* October 29, 2019, https://www.washingtonpost.com/opinions/2019/10/29/why-whatsapp-is-pushing-back-nso-group-hacking/.

[4] Lily Hay Newman, ”If China Hacked Mariott, 2014 Marked a Full-on Assault,” *Wired,* December 12, 2018, https://www.wired.com/story/marriott-hack-china-2014-opm-anthem/.

[5] Justin Ling, “Man Who Sold F-35 Secrets to China Pleads Guilty”, *Vice News*, March 24, 2016, https://www.vice.com/en_us/article/kz9xgn/man-who-sold-f-35-secrets-to-china-pleads-guilty.

[6] Sherisse Pham, “Chinese wind turbine firm found guilty of stealing U.S. secrets,” CNN Business, January 25, 2018, https://money.cnn.com/2018/01/25/technology/china-us-sinovel-theft-conviction/index.html.

attacks, including recruiting insiders to steal from their companies or provide access to protected networks.

Finally, nation states have used offensive cyber capabilities to launch disruptive and destructive cyber attacks to coerce and threaten the United States and US companies. For example, from 2012-2014, Iranian hackers launched a series of massive Distributed Denial of Service (DDoS) attacks on US financial institutions[7] after the release of a controversial film that depicted the prophet Muhammad, and to put pressure on the USG during negotiations over the Iranian nuclear program. In November 2014, North Korean hackers attacked Sony Pictures over the release of a Seth Rogen movie making fun of North Korean Supreme Leader Kim Jong Un.[8]

Cybercrime has also grown significantly, driven by the development of a complex and diverse criminal ecosystem that has increased the capabilities of leading cybercriminal syndicates and lowered the barriers to entry for unsophisticated actors. In 2018, CSIS estimated that cybercrime cost the global economy more than $600 billion dollars, or nearly 1% of global GDP, up 35% from 2014.[9]

The growth of cybercrime around the world can be linked to three broad trends. First, advanced tools and techniques formerly available only to the most sophisticated nation-states have become available to criminals. This is driven in part by the blurry line between criminal and nation-state hacker groups, particularly in Russia and Eastern Europe,[10] partly by the leaking of advanced hacking tools by groups like the Shadow Brokers,[11] and partly by "grey market" vendors who hire former hackers from intelligence services like NSA, GRU and Mossad to develop hacking tools for sale. While many of these tools and techniques are not necessarily available to a small-time hacker, they have fueled the growing scale and ambition of attacks by sophisticated criminal syndicates.

Second, the development of a mature, dynamic underground economy has transformed the cybercrime ecosystem. As the underground market has evolved and become more transparent, it has become highly competitive, driving fast-paced innovation by black hats and leading to the emergence of a market for cybercrime-as-a-service that has allowed unsophisticated actors to assemble highly lucrative criminal campaigns at little cost with minimal risk.[12] Where

[7] "Operation Cleaver," Cylance, December 2014, https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf.

[8] David E. Sanger and Nicole Perlroth, "U.S. Said to Find North Korea Ordered Cyberattack on Sony," *The New York Times*, December 17, 2014, https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0.

[9] James A. Lewis, "Economic Impact of Cybercrime – No Slowing Down," Center for Strategic and International Studies, February 21, 2018, https://www.csis.org/analysis/economic-impact-cybercrime.

[10] Michael Schwirtz and Joseph Goldstein, "Russian Espionage Piggybacks on a Cybercriminal's Hacking," *The New York Times*, March 12, 2017, https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html.

[11] Swati Khandelwal, "Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs," *The Hacker News*, April 22, 2017, https://thehackernews.com/2017/04/windows-hacking-tools.html.

[12] "Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity," Center for Strategic and International Studies, February 2017, https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/other-projects-cybersecurity-0.

committing a complex cybercrime campaign used to require significant resources and a combination of specialized technical skills, today a would-be criminal can buy all the necessary parts of a criminal campaign online for a few hundred dollars: off-the-shelf exploit kits and malware payloads to commit the actual attack, phishing services to reach potential victims, 24/7 customer service to help configure tools and fix bugs, compromised servers and infrastructure to launch the attack and exfiltrate stolen data, and money-laundering and mule services to get clean cash delivered to the attacker's bank account.

Finally, law enforcement's inability to keep up with changes in technology has made cybercrime virtually consequence-free. Anonymization tools, digital wallets and cryptocurrencies, easy-to-use encryption, and polymorphic and partially automated malware have not only made cybercrime easier and cheaper, they have made law enforcement's job nearly impossible. A study by Third Way found that only 0.3% of *reported* cyber attacks in the US result in an arrest, and cybercrime is already massively underreported.[13] That number is likely significantly lower around the world, particularly in developing countries with little to no law enforcement capacity to investigate digital crimes. Law enforcement's challenge has only grown with the proliferation of cybercrime tools and services in the underground market. Even when attacks can be linked to broader campaigns and tools and techniques can be identified, linking any one of the many vendors and criminals in the underground ecosystem that offer that tool or service to a specific crime is nearly impossible.

It is no surprise, therefore, that despite much higher awareness of cyber threats by businesses and consumers and significant investments in cyber defense in recent years, cybercrime continues to be a booming business. Wider access to vulnerabilities, exploits and tools, efficient markets that reduce the money and skills needed to engage in cybercrime at scale, and a near-total lack of consequences for those engaged in criminal activity mean that the risk/reward tradeoff continues to draw talent and investment into cybercrime.

Lawful Exploitation of Data by Governments

Cyber attacks are just one of many threats to private and sensitive data. In many ways the more troublesome challenge for US companies is the growth of *lawful* exploitation of technology and data by governments. "Lawful exploitation" is the collection and use of data by governments through legal mechanisms but with potentially harmful consequences. US companies are increasingly global, and the major US technology platforms, in particular, find themselves caught between their internal policies and ethics and the demands of global governments to facilitate surveillance, intelligence collection, and law enforcement.

What makes this challenging for companies is that fact that many of these demands, on the surface at least, are not unreasonable. Countries wish to enforce their laws and protect their citizens (as they define both of these goals), and expect companies that do business in their countries to enable them to do so. Three key problems arise for companies.

[13] Mieke Eoyang et al., "To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors," Third Way, October 29, 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors.

The first is when countries lack effective governance mechanisms to prevent inadvertent or surreptitious abuse of legally disclosed data. For example, many countries around the world lack independent judicial review of search warrants, meaning that, even if the vast majority of search warrants are issued by legitimate law enforcement officers investigating serious crimes, there are few checks in place to prevent a false or unreasonable warrant from being used to access a customer's data for malicious purposes.

The second set of issues are caused by cultural differences between US companies with American values and their global customers. This problem is perhaps most prevalent in content management, where US social media platforms allow users to post a wide variety of content based on US concepts of free speech that are considered illegal and insulting in other parts of the world, for example under lese-majeste or political speech laws. But cultural differences don't just have to do with content. Balancing their desire to promote the free and open flow of information with the cultural sensitivities and legal regimes of the countries in which they operate is one of the leading global challenges for US technology companies.

The third is the exploitation of data and technology by governments engaged in malicious surveillance, repression, and exclusion. Countries like China have strict laws governing online speech and are utilizing tools like facial recognition, drones and biometric scanners to monitor and detain minority groups in the western province of Xinjiang. Companies that operate in China may have no choice but to censor and identify users engaged in political speech and provide the government with nearly unfettered access to their data if asked, and companies who sell these technologies to China may be knowingly or unknowingly enabling human rights abuses.

US companies and the USG have developed a range of technologies and policies to combat these challenges. For many companies, the most powerful tool in their arsenal to protect their users' data from lawful exploitation by governments is unrecoverable encryption. If the company lacks the technical capability to decrypt the data, they cannot provide it to foreign governments, even when served with a legal order. The implementation of end-to-end encryption (E2EE) by platforms like WhatsApp, for example, prevent Facebook (which owns WhatsApp) from sharing the content of users' communications with foreign governments. Ephemerality is another increasingly popular tool that companies use to avoid disclosing customer data to governments. Companies like Wickr simply delete the data so that there is nothing for governments to take. The USG has also helped companies to avoid disclosing data, for example through the Electronic Communications Privacy Act (ECPA) which prevents US companies from disclosing the content of communications stored in the United States to a foreign government unless that government submits a Mutual Legal Assistance (MLA) request through the US government.

But this approach has significant costs and tradeoffs. Implementing technical solutions that prevent them from disclosing data to governments in order to prevent abuse is great, except that it can also prevent companies from providing data that could prevent serious crimes or terrorism. The rollout of E2EE on Facebook Messenger, for example, will render most of the tools currently used to identify and report child pornography on the platform ineffective, a serious problem since Facebook is the number one reporter of child exploitation content to the National Center for Missing and Exploited Children (NCMEC).[14]

And online crimes are not the only types of crimes being impacted. Growing challenges to accessing digital evidence, whether due to encryption, ephemerality, cross-border access issues, or simply the opacity and complexity of the digital ecosystem have imperiled global law enforcement's ability to investigate conventional crimes as well, including serious crimes like murder, rape, drug trafficking and burglary. It is not just repressive and autocratic states that suffer, but liberal democracies, including the US.

Regulatory and Policy Risks to Innovation, Competition and Data Protection

The growing tension between companies and governments has led to the rise of another significant risk to US companies: the adoption of counterproductive policies by foreign governments seeking to exercise their sovereignty over technology and data that harm innovation, competitiveness and economic growth. As more companies implement unrecoverable encryption, delete customer data, move data across national borders, and fail to meet the demands of governments for data, the inability to enforce their laws and exercise their sovereignty over their citizens and their data is increasingly unacceptable to governments. In response, there is a growing trend of regulations and policies placing mandates on technologies and businesses in order to ensure the government's ability to access and utilize data. Some of these mandates can create significant costs and constraints for companies, with negative effects on innovation, competition, and data protection. Other countries have turned to lawful hacking, developing offensive cyber capabilities or hiring grey market vendors to exploit vulnerabilities in widely used systems without oversight or accountability to gain access to the data they need.

For many countries, the first step in exercising greater control over their citizens' data is to implement data localization mandates. Our understanding of jurisdiction and sovereignty is based on thousands of years of analog law and policy, and controlling the physical location of data often makes it easier for governments to enforce their own laws about how that data is collected, stored, secured and used.

Data localization policies come in two forms: requirements that companies store data on physical infrastructure within the country's borders, and restrictions on the flow of data across the country's borders. Requirements for domestic storage are more common and are not entirely new. While they have become far more common in recent years, with new data localization mandates introduced in countries like Russia, India, and South Africa (among many others), many have been in place for a long time, particularly restrictions on certain types of data. As an example, both the US and Germany have long required certain financial data to be stored

[14] Casey Newton, "Encrypted messaging is becoming more popular, and child advocates are worried," *The Verge*, September 13, 2019, www.theverge.com/facebook/2019/9/13/20863489/encryption-stanford-conference-facebook-ncmec-ghq.

domestically for auditing purposes. Restrictions on cross-border data flows are less common. Under Europe's General Data Protection Regulation (GDPR), companies must meet strict standards in order to transfer data outside of the EU, while China bars companies from transferring certain data outside the country entirely.[15]

Both forms of data localization create significant problems for US companies. At the simplest level, laws that require domestic storage of data require companies to build or partner with data centers on the ground in country. Restrictions on data flows can further force them to localize actual business functions in a country, in addition to the data itself. This creates unnecessary costs and inefficiency for companies, and can create operational challenges as it forces them to segregate data on the back end to ensure that it is kept within the appropriate jurisdictions.

Data localization can also make it difficult to protect data from government abuse. Having physical access to technology allows governments to use a much wider range of techniques to access and exploit that data, from malicious insiders to exploiting hardware, in ways that are impossible to do remotely.

Data localization can also subject companies to data retention mandates and restrictions on encryption that apply within the country's borders. Data retention mandates require companies to store data for a specified period of time, often to facilitate government access. In some cases they are industry or application specific. In the US, for example, the FCC requires phone companies to store your phone records for at least 18 months for law enforcement purposes. Data retention mandates are not new (the FCC rule dates back to legislation from 1986),[16] and have faced significant pushback from courts in many countries. For example, high profile court decisions invalidated the EU's Data Retention Directive[17] and the UK's Data Retention and Investigatory Powers Act[18] in 2014 and 2016. Data retention mandates present significant risks to companies and their customers' data. If companies cannot delete sensitive data, it can be inadvertently exposed, targeted by hackers, accessed inappropriately by employees, or demanded by governments.

Finally, governments are increasingly pursuing mandates that limit how companies secure their users' data in order to ensure government access. Perhaps the most contentious of these mandates are restrictions on the use of encryption. Encryption is an essential cybersecurity tool. Data that is encrypted is protected from abuse even if a malicious actor gains access to a company's systems.

[15] James A. Lewis, Denise E. Zheng, and William A. Carter, "The Effect of Encryption on Lawful Access to Communications and Data," Center for Strategic and International Studies, February 2017, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170221_Lewis_EncryptionsEffect_Web.pdf.

[16] "47 CFR § 42.6 – Retention of telephone toll records," Cornell Law School Legal Information Institute, https://www.law.cornell.edu/cfr/text/47/42.6.

[17] "European Union: ECJ Invalidates Data Retention Directive," Library of Congress, June 2014, https://www.loc.gov/law/help/eu-data-retention-directive/eu.php.

[18] "MPs win surveillance powers legal challenge," BBC News, July 17, 2015, https://www.bbc.com/news/uk-politics-33564442.

But certain forms of encryption, particularly end-to-end encryption of data in motion (E2EE) and full-disk encryption of data at rest (FDE) also create problems for law enforcement and intelligence agencies seeking to access data. E2EE and FDE refer to forms of encryption that cannot be decrypted except with the user's unique key. Importantly, while most digital data is now encrypted, *the vast majority is not protected by E2EE or FDE*. Most data is encrypted using "recoverable encryption" techniques that allow companies to decrypt users' data under certain circumstances, usually for the user's benefit. For example, virtually all email is encrypted using recoverable encryption because if users forget their passwords they want companies to be able to restore access to their accounts. Almost all businesses use encryption that allows for access to users' data so that when an employee leaves the company access to data is not lost, or to ensure that employees comply with company policies.

E2EE and FDE are almost exclusively used in two specific applications: instant messaging and smart phones. In recent years, the largest instant messaging platforms outside of China, WhatsApp and Facebook Messenger (both owned by Facebook), iMessage and Viber, have implemented E2EE by default, and smaller services that offer E2EE like Signal and Threema have grown in popularity. At the same time, both iOS and Android, the two OS families used on almost every smart phone in the world, have implemented FDE by default. When governments request access to these companies' users' communications, the companies are unable to comply, even if the request is made through appropriate legal process.

The impact on government access to communications has been profound. Around the world, law enforcement and intelligence agencies have raised the alarm about digital evidence "going dark," or becoming increasingly inaccessible to law enforcement because of changes in technology. Without access to communications between criminals, investigating and successfully prosecuting many types of crimes has become nearly impossible. In response, many governments around the world, including the UK and Australia, have passed new laws empowering them to order companies to maintain the capability to facilitate lawful access to communications.

Restricting the use of tools like encryption and ephemerality to secure data creates its own significant challenges. First, it requires companies to maintain some sort of access mechanism to encrypted communications that they have to secure against attack. Any "master key" or "repository of keys" becomes a magnet for attackers who want to be able to access user data at scale, and the burden of protecting these access mechanisms falls on companies.

Not only does this limit the tools companies can use to protect their customers' data, it has a disproportionate impact on small and medium enterprises (SMEs) that harms competition. Google, for example, may have the resources and talent to fight off an APT trying to exploit Gmail, but startups with tiny staffs that quickly scale to serve millions of customers (e.g. WhatsApp in its early days) do not. With the cost of lawsuits and regulatory fines for data breaches growing every year, trying to secure an access point for law enforcement could become an untenable liability to small companies.

This threat is further fueled by the growing reliance of governments on "lawful hacking" to access data that is no longer available through service providers. Faced with the inability to access digital evidence through lawful process, law enforcement and intelligence agencies increasingly rely on legal authorities that allow them to exploit vulnerabilities in hardware and software to bypass security measures and access data. In fact, some researchers and advocates have gone so far as to argue for a shift in the law enforcement model from "building vulnerabilities into systems" to exploiting vulnerabilities that are already there.

This is a fundamentally flawed approach that should be discouraged. Lawful hacking is by necessity opaque and unaccountable. If governments reveal their techniques and the vulnerabilities and exploits that they use to access data through lawful hacking, vendors will patch those vulnerabilities, rendering these tools ineffective. Lawful hacking is expensive and time consuming and requires significant technical resources and expertise, and law enforcement agencies around the world already struggle with significant resource constraints. Finally, and most importantly, promoting the use of lawful hacking by governments creates incentives that undermine global cybersecurity. It encourages more governments around to develop or acquire offensive cyber capabilities, fuels the growth of "grey market" firms like NSO group that are linked to ethically and legally questionable activities that threaten human rights and civil liberties, and discourages the disclosure of exploitable vulnerabilities to vendors so that they can be patched.

And it is not just malicious access that poses challenges to innovation and competition. Complying with law enforcement requests for data is difficult and costly for companies. US law enforcement submits nearly 70,000 requests for data to the six largest US technology platforms alone, and all of those requests are in English and submitted under US legal standards.[19] Meeting the needs of thousands of law enforcement agencies across hundreds of countries in dozens of languages under the current system is simply infeasible for many companies, and further burdens SMEs trying to break into these markets with overhead and liability. Reduced competition and increased costs, in turn, harm innovation, reducing incentives for and resources to support R&D.

What Can US Policymakers Do to Address These Challenges?

The US government must play a leading role in addressing the many threats to data security both lawful and unlawful, around the world. The United States is home to the world's largest and most competitive technology platforms, which are responsible for protecting much of the world's sensitive data. Our economy depends in large part on the competitiveness and innovation of our technology industry, and our national security is built on technical and information dominance.

[19] William A. Carter and Jennifer C. Daskal, "Low Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge," Center for Strategic and International Studies, July 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf.

That does not mean that the USG can or should go it alone. The internet, and the US technology platforms that dominate it, are fundamentally global, and our approach to data governance and protection must reflect that. But US leadership will be essential to protect our economic and national security interests, and to promote the development of a healthy, free, open, safe and positive internet for all. The USG must continue to build on the progress of the last decade to strengthen cyber defenses and shape incentives and impose consequences on malicious actors. We must also empower law enforcement and facilitate appropriate and lawful access to data for governments, and push back on policies that seek access to data at the expense of security, innovation and competition.

Strengthen Cyber Defenses and Rebalance Incentives for Attackers and Defenders

Cybersecurity has progressed dramatically, driven by broader awareness, new security technologies, significant investment, and the growth of the private cybersecurity industry. Cybersecurity spending in the US grew has more than doubled since 2010, from $27.4 billion to $66 billion last year,[20] and in many ways the cyber defense landscape is nearly unrecognizable. A dedicated CIO or CISO has become the norm for many companies, boards and C-suite executives are routinely briefed on cybersecurity, and basic security practices like authentication, encryption, security training, antivirus protection, and information sharing are widespread.

USG leadership deserves much of the credit for this progress. Executive Order 13636,[21] released by the Obama Administration in 2013, created significant changes in the way that we protect critical infrastructure, establishing the critical infrastructure sectors, reorganizing how the USG approaches cybersecurity, encouraging regulators to hold companies accountable for implementing basic security practices, and incentivizing companies to collaborate with each other and the government to combat cyber threats. The development of the NIST Framework[22] established a common baseline for how companies and governments around the world think about cyber resilience. Perhaps most importantly, it broadened the way that senior leaders think about cyber risk management from a purely technical issue to how technology, people and governance all contribute to security.

But more needs to be done. In 2015 CSIS convened a Cyber Policy Task Force for the 45th President[23] to strengthen cybersecurity for the US. Its key recommendations remain relevant today. Despite progress, many companies still fail to implement baseline cybersecurity practices

[20] Statista Research Department, "Spending on cybersecurity in the United States 2010-2018," Statista, August 9, 2019, https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/.

[21] "Executive Order – Improving Critical Infrastructure Cybersecurity," The White House, Office of the Press Secretary, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[22] "Framework for Improving Critical Infrastructure Cybersecurity," National Institute for Standards and Technology, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[23] "CSIS Cyber Policy Task Force," Center for Strategic and International Studies, January 2017, https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/other-projects-cybersecurity-2

and cyber hygiene, and this continues to be the source of most breaches and cyber attacks. The NIST Framework is necessary but not sufficient to establish effective protection for national critical infrastructure. The Framework is broad and theoretical, serving as a good foundation for establishing a macro strategy for cybersecurity across the diverse range of stakeholders and networks that make up cyberspace. It does not, however, do very much to help a specific company or individual to understand the micro decisions necessary to secure their data online, nor does it lend itself to the development of concrete metrics or standards that can serve as a basis for regulatory oversight and enforcement.

The USG should supported continued collaboration between NIST and the private sector to build concrete implementation guidance and metrics for adoption and effectiveness of the Framework. This can facilitate voluntary investments in cybersecurity by companies and, where necessary, regulatory mandates to ensure that our critical infrastructure is protected.

The USG should also increase penalties for companies that fail to protect their users' data, and for vendors that fail to build robust security into their products and services. Companies continue to underinvest in cybersecurity because of uncertain returns on investment. For many companies, absorbing the hypothetical cost of a breach remains an economical alternative to the real cost of establishing and maintaining strong cyber defenses. Increased regulatory penalties and civil liability can raise the cost of security failures for companies, incentivizing them to spend more on defense. And this should not just be applied to companies that collect and use customer data. Vendors must also be held accountable for building robust security into their products and services, particularly vendors of connected devices that make of the Internet of Things (IoT), which are a fast-growing threat vector.

The USG can also play a role in addressing resource gaps that stand in the way of improved security outcomes. Talent, in particular, remains a significant challenge for cyber defenders. Not only do companies struggle to attract enough skilled cyber defenders, but the education and training system does a poor job of aligning the skills it provides with the actual needs of employers. The USG should invest in an ambitious education and workforce plan for cybersecurity, with a system for accrediting training and educational institutions; a taxonomy of cybersecurity roles and the skills that practitioners must demonstrate to claim competence in each specialty; and a robust network of professional credentialing entities.

Strengthening defenses alone is not enough. Creating consequences for malicious actors is the most effective way to reduce cyber risk. The sophistication and determination of APTs make it very difficult, if not impossible, to prevent them from exploiting our government networks and critical infrastructure through defensive measures alone. Defenders must defend the entire network 100% of the time, but attackers need only find one flaw in those defenses that allows them to achieve their goals. Protecting ourselves against these threats requires a combination of deterrence and international norms and agreements to shape incentives for nation-states and their proxies so that they choose to use their cyber capabilities responsibly and not to launch attacks on the US.

The USG has helped to drive significant international progress. Norms of state behavior in cyberspace, while imperfect and incomplete, have come a long way in the last decade. Two UN Groups of Government Experts (GGEs) released cyber norms in 2013[24] and 2015[25] with the support of all of the major cyber powers, covering many of the key risks to global networks, for example forswearing attacks on civilian critical infrastructure in peacetime. Broad principles that might seem obvious, but were once the subject of debate, have been settled, for example that international law applies in cyberspace, as does national sovereignty (although exactly what these terms mean and *how* they should be applied remains a question). The Tallinn Manual was released in 2013[26] and updated in 2017[27] outlining expert views from around the world on the applicability of international law, particularly the laws of armed conflict, to cyber operations. The Budapest convention on Cybercrime,[28] originally developed in 2001, has been ratified by 64 countries.

Progress on international norms has stalled in recent years, with the 2017 UNGGE failing to reach agreement on advancing cyber norms, but efforts are ongoing. The Global Commission on the Stability of Cyberspace (GCSC)[29] was established by the Netherlands in 2017 to bring together leading experts to advance a common global understanding of cyber issues. Last November, French President Emmanuel Macron introduced the *Paris Call for Trust and Security in Cyberspace*,[30] a set of principles aimed at breaking the deadlock between leading cyber powers and achieving broad consensus on additional norms, but the US, Russia and China have not signed it. A new GGE has been convened at the UN, and at Russia's request a parallel Open Ended Working Group (OEWG), opening up debates around cyber norms to the full membership of the UN.

Deterrence has also advanced significantly. Ten years ago, the US had no clearly articulated deterrence framework for cyber attacks. Since the initial release of the Obama Administration's

[24] "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations General Assembly, June 24, 2013, https://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

[25] "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations General Assembly, July 22, 2015, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

[26] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, February 2013) https://www.cambridge.org/us/academic/subjects/law/humanitarian-law/tallinn-manual-international-law-applicable-cyber-warfare?format=AR#contentsTabAnchor.

[27] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, February 2017) https://www.cambridge.org/us/academic/subjects/law/humanitarian-law/tallinn-manual-20-international-law-applicable-cyber-operations-2nd-edition?format=PB.

[28] "Convention on Cybercrime," European Treaty Series No. 185, Council of Europe, November 23, 2011, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

[29] "Launch of Global Commission on the Stability of Cyberspace," Global Commission of the Stability of Cyberspace, February 18, 2017, https://cyberstability.org/news/launch-of-global-commission-on-the-stability-of-cyberspace/.

[30] "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace," French Diplomatie, Ministry for Europe and Foreign Affairs, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World[31] and *Department of Defense Strategy for Operating in Cyberspace*[32] in 2011, US cyber deterrence doctrine and capabilities have evolved significantly. Today, the United States has outlined definitions of the cyber threats to data, access, property and people that we seek to deter and the range of tools we will use to impose consequences on attackers. The USG has invested significant effort in building our toolkit to investigate and respond to these attacks, developing our capacity to use all-source intelligence to effectively attribute major attacks and to utilize everything from sanctions and indictments to cyber and kinetic retaliation to impose costs on attackers.

Yet norms, capabilities and doctrine can only go so far in the absence of clear political will to impose consequences on malicious actors. Attribution and cost imposition are key to deterring foreign nation-states from attacking the US and enforcing norms of state behavior, but both the Obama and Trump administrations have repeatedly demonstrated a lack of resolve to forcefully and publicly identify and punish foreign adversaries that violate norms of state behavior in cyberspace. International relationships are complex and multifaceted, but allowing dangerous adversaries like Russia, China, Iran and North Korea to attack critical infrastructure and steal data with few consequences out of a desire to pursue broader agreements on trade and security simply encourages other countries to develop similar capabilities and engage in malicious behavior.

Part of the problem is the opacity of cyberspace and the difficulty of enforcing norms of state behavior. The problem is no longer the ability to attribute attacks, at least for the USG, but the ability to convince partners and adversaries, as well as the public, of our attribution in order to legitimize retaliatory measures and hold countries accountable for complying with international norms. US intelligence agencies, and even the private cybersecurity industry, have become quite adept at identifying perpetrators of cyber attacks, especially leading APTs, but we struggle to share evidence of attribution because of concerns about exposing our sources and methods. The USG must develop a consistent and transparent approach to attribution, as well as channels to safely and credibly share details of attribution with allies, partners, adversaries and the public.

Imposing severe consequences on cybercriminals is also essential. Cybercrime has become an epidemic, and we have consistently failed to empower law enforcement to combat the problem. Addressing the scourge of cybercrime around the world is a huge task. The simplest is addressing law enforcement's significant resource constraints. Investigating cybercrimes is complex and time consuming, requiring technical tools and specialized skills. The USG should ensure that law enforcement agencies from the municipal to the global level get the resources necessary to build and maintain the tools and workforce to effectively combat cybercrime.

[31] *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, D.C: The White House, May 2011) https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[32] *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011) https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Empower Law Enforcement and Facilitate Appropriate and Lawful Access to Data for Governments

Cybercrime is just one small piece of the law enforcement puzzle. Many of the most significant threats to data protection, innovation and competition around the world come from governments' growing frustration with a status quo in which they are unable to access the data that they feel they need to enforce their laws, exercise their sovereignty, and secure their national interests. If the US continues to stand on principle and refuse to work toward compromises that at least partially address other countries' needs and preferences, those countries will continue to pursue policies like market access barriers, data localization, data retention and encryption mandates that harm US companies and undermine global data security.

Technology challenges to government access to data are complex and many faceted. To start, we can break down the challenges that governments face into a few broad buckets. First is accessing data across borders, particularly for law enforcement purposes. Second is architectural and technical measures implemented by companies to secure user data that make it difficult or impossible for governments to access data through traditional means. The final challenge, which is perhaps both most important and least appreciated, is the unnecessary and counterproductive friction between companies and governments due to information asymmetry, differences of values, and gaps in legal frameworks.

The MLA system which facilitates cross-border law enforcement access to data is fundamentally broken and must be replaced. It is too slow, costly, and difficult to use to be effective. The USG should take the lead in eliminating the MLA system and establishing a new regime for international evidence collection which is efficient, scalable, and builds in transparency, accountability and protections for civil liberties. The CLOUD Act is a good start, and the USG should prioritize the negotiation of CLOUD Act agreements with foreign partners, both by incentivizing them to implement legal reforms and finding ways to accommodate the different legal customs and practices of other countries while also ensuring that privacy and civil liberties are respected.

The implementation of security measures like encryption and ephemerality by primarily US companies has transformed the digital landscape for governments. Tools that law enforcement has relied on for decades, from wiretaps to calling records, location data, and accessing text messages have become increasingly unreliable. It is difficult to believe that this has not had a negative impact on combatting crime, terrorism, and espionage. On the other side, protecting private and sensitive data is incredibly important, and ensuring that US technology is not used in ways that harm marginalized and at-risk communities is essential to maintaining US leadership and values in the world.

Debating the appropriate balance of equities between privacy and data protection, on one hand, and rule of law and public safety on the other has become a fraught debate increasingly founded on incomplete and anecdotal data. The USG must take the lead in building a foundation of knowledge of this domain on which future debates around how we secure digital data and communications can be based. Do marginalized groups, activists, human rights defenders, and political dissidents actually use encryption and ephemerality to protect themselves from repressive regimes? Is it actually effective in protecting these communities? How much has the implementation of these measures improved security outcomes for users of the major technology platforms? How big of a challenge is this for law enforcement and intelligence agencies, and what are the costs in terms of crime and threats to public safety from the resulting failures? Do the measures that governments are taking to compensate for their inability to access data through traditional means actually lead to worse outcomes for privacy and civil liberties? This data simply does not exist, and without it we cannot move the debate forward. The USG must leverage a combination of funding, incentives and mandates to ensure that this data is collected, analyzed and disseminated.

Once we develop data around the impact of these measures we must engage in a substantive, respectful and pragmatic debate about how to balance these equities that is based on the reality of the world that we live in, not the ideal worlds in which we wish we lived. We must put aside our biases and be open to all possible approaches, and recognize that all parties to this debate come to it with the best of intentions, even if they have widely different world views. Both the "encryption and ephemerality can never be compromised" and the "companies must always provide data pursuant to legal process" camps must come to the table willing to make concessions to reach better outcomes.

Perhaps the most important thing that the USG can do, however, is to take steps to ease the unnecessary and counterproductive friction between governments and companies that hold the data that they want. I partnered with a professor from American University, Jennifer Daskal, to conduct a multi-year study of law enforcement's challenges with digital evidence in which we conducted surveys, interviews, and roundtables with hundreds of law enforcement representatives across the United States.[33] The results were surprising. As much as cross-border access, encryption and ephemerality are serious challenges to law enforcement, the biggest problems for law enforcement are actually understanding what data is out there, which providers have access to what data, what the appropriate legal process is to acquire it, and how to make use of that data once they receive it. Conversations with international law enforcement partners have confirmed that this pattern holds around the world.

Our study, Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge, outlined a series of recommendations to Congress, law enforcement, attorneys and judges, and service providers to help ease the tension between providers and law enforcement and facilitate the smooth and efficient exchange of information. Greater resources, clear legal authorities, points of contact and communication mechanisms, improved transparency and education and training for law enforcement, and concrete and consistent policies for the collection and use of data by governments are needed to reestablish these relationships on a stronger footing.

The study received the support of members of every stakeholder group, including law enforcement officials from DoJ to local police, members of Congress, national security leaders, international partners, leading technology companies, and civil society organizations. The USG

[33] William A Carter and Jennifer C. Daskal, "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge," Center for Strategic and International Studies, July 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf.

should work to implement the findings of the study to ease the burden on governments and reduce incentives for them to pursue counterproductive policies to maintain access to data.

Finally, the USG should push back on governments that exploit data and technology in harmful and dangerous ways. If we offer a path forward that facilitates appropriate government access to data and enables governments around the world to protect their citizens and enforce their laws, we can effectively argue against policies that seek to fill these gaps in harmful ways. Data localization, technology mandates, and restrictions on market access harm US companies, undermine innovation and competition in the global technology industry, and risk the security of private and sensitive data of individuals and companies around the world.

I thank the Committee for the opportunity to testify, and look forward to your questions.