SUBMITTED STATEMENT OF

BRANDON J. PUGH, ESQ.
POLICY DIRECTOR & RESIDENT SENIOR FELLOW,
CYBERSECURITY & EMERGING THREATS
R STREET INSTITUTE

BEFORE THE

SUBCOMMITTEE ON INNOVATION, DATA, AND COMMERCE
COMMITTEE ON ENERGY AND COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

HEARING ON

ECONOMIC DANGER ZONE: HOW AMERICA COMPETES TO WIN THE FUTURE VERSUS CHINA

FEBRUARY 1, 2023

ECONOMIC DANGER ZONE:
HOW AMERICA COMPETES TO WIN THE FUTURE VERSUS CHINA

STATEMENT SUMMARY

I. A comprehensive data privacy and security law offers benefits to consumers and industry. There is also a strong nexus between privacy and security. Both of these necessitate a privacy law being a priority of the 118th Congress.

II. The Chinese Communist Party (CCP) has a history of widespread data collection on its citizens and individuals worldwide, including Americans. Data in the hands of an adversarial nation-state or a malicious actor can lead to devastating consequences.

III. There are ways to help mitigate and reduce these concerns, even though China's collection and abuse of data is likely never going to end. A national data privacy and security law, like the American Data Privacy and Protection Act (ADPPA) from the 117th Congress, is the most logical next step.

IV. There are multiple benefits of a comprehensive data privacy and security law that could help address the data collection crisis, including: making America more competitive; implementing provisions that help minimize privacy and security threats; and addressing broader concerns around software, hardware and applications with a nexus to China.

ECONOMIC DANGER ZONE:
HOW AMERICA COMPETES TO WIN THE FUTURE VERSUS CHINA

Chairman Bilirakis, Ranking Member Schakowsky and members of the Subcommittee:

Thank you for considering my testimony and for the invitation to speak at this hearing. My name is Brandon Pugh and I am the policy director of and resident senior fellow for the Cybersecurity and Emerging Threats team at the R Street Institute, which includes our data privacy and data security portfolio. The R Street Institute is a nonprofit, nonpartisan, public policy research organization, whose mission is to engage in policy research and outreach to promote free markets and limited, effective government.

In addition to leading our team, my personal research focuses on finding consensus on a comprehensive federal data privacy and security law in the United States. We published a report last year in conjunction with the Harvard Kennedy School's Belfer Center to provide recommendations that address some of the most challenging aspects of a federal data privacy and security law.[1] Our research included consultations with over 125 entities of varying ideologies. One key aspect of our ongoing work is the intersection of privacy and security, including how national security and data security should be key drivers in passing a federal law. That is why today's hearing is of special interest to us.

Let me begin by personally thanking the subcommittee and the members of the entire Energy and Commerce Committee for the time dedicated to the American Data Privacy and Protection Act (ADPPA) last Congress. Notably, the leadership of Chairwoman Cathy McMorris Rodgers and Ranking Member Frank Pallone.

[1] Tatyana Bolton et al., "The Path to Reaching Consensus for Federal Data Security and Privacy Legislation," R Street Institute, May 26, 2022. https://www.rstreet.org/2022/05/26/the-path-to-reaching-consensus-for-federal-data-security-and-privacy-legislation.

Data privacy and security are vital to both consumers and industry. Consumers would benefit from a national privacy law by having protections and rights surrounding their data regardless of their state of residence. Unfortunately, only the residents of five states will enjoy any such protections in 2023.[2] Similarly, data privacy and security laws would benefit industry by providing certainty, clarity and uniformity instead of a patchwork of state-level privacy laws.[3] So far, at least 39 states have considered comprehensive privacy laws since 2018, and I expect this to expand.[4]

In addition to the benefits to consumers and industry, such a law is vital to our national security. This often underappreciated aspect of data privacy and security will be the focus of my testimony today. Given the topic of today's hearing, I will focus my analysis on the context of China.

In 2020, the China Task Force found that the Chinese Communist Party (CCP) "has a record of using official government resources and companies with CCP affiliations to compromise the data of people around the world" and that the United States and its allies need to join the "effort to secure data from the CCP's surveillance state and other malign entities."[5] These concerns are especially prevalent in China itself, where advanced technology is used to track and monitor their citizens with few protections.

Similar concerns are echoed by federal government leaders like Federal Bureau of Investigation Director Christopher Wray, who previously said "if you are an American adult, it is

---

[2] Anokhy Desai, "US State Privacy Legislation Tracker," International Association of Privacy Professionals, Jan. 27, 2023. https://iapp.org/resources/article/us-state-privacy-legislation-tracker.
[3] Tatyna Bolton et al., "Preemption in Federal Data Security and Privacy Legislation," R Street Institute, May 31, 2022. https://www.rstreet.org/2022/05/31/preemption-in-federal-data-security-and-privacy-legislation.
[4] "Privacy Matters in the US States," International Association of Privacy Professionals, Jan. 28, 2023. https://iapp.org/media/pdf/resource_center/infographic_privacy_matters_in_the_us_states.pdf.
[5] Michael McCaul et al., *China Task Force Report*, U.S. House of Representatives, September 2020. https://foreignaffairs.house.gov/wp-content/uploads/2020/11/China-Task-Force-Final-Report-11.6.20.pdf.

more likely than not that China has stolen your personal data."[6] He made even more pointed comments recently, saying that "China's vast hacking program is the world's largest, and they have stolen more Americans' personal and business data than every other nation combined."[7]

I wish I could say that the concerns raised during the 116th Congress are no longer valid. In fact, the opposite is true—it is worse. Data, in general, can reveal everything from your shopping habits to sensitive parts of your life like your health and location. This, in the hands of an adversary or malicious actor, can have devastating consequences, especially for vulnerable populations. Americans are not naïve to this threat. They understand their personal data is not secure, but they believe they are powerless to fix it.[8]

As one recent example in the Russia-Ukraine war highlights, data can even be amassed to target disinformation campaigns or direct even physical violence toward those in conflict.[9] This is certainly not an isolated capability and is an issue that the United States should worry about. Data can even be synthesized to help identify intelligence agents and "stymie U.S. efforts to cultivate sources of information and influence around the world."[10] It goes without saying that the United States' rivalry with China has taken on a digital nature and China has been in a race with us in

---

[6] Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States," Hosting Entity: Hudson Institute, July 7, 2020. https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.

[7] Chloe Folmar, "FBI head: China has 'stolen more' US data 'than every other nation combined'," *The Hill*, Nov. 15, 2022. https://thehill.com/policy/cybersecurity/3737251-fbi-head-china-has-stolen-more-us-data-than-every-other-nation-combined.

[8] Brooke Auxier et al., "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," Pew Research Center, Nov. 15, 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information.

[9] Jessica Dawson and Brandon Pugh, "Ukraine conflict heightens US military's data privacy vulnerabilities," *Defense News*, April 14, 2022. https://www.defensenews.com/opinion/2022/04/14/ukraine-conflict-heightens-us-militarys-data-privacy-vulnerabilities.

[10] Matt Gimovsky et al., "Congress Needs to Start Caring About Our Privacy as Much as China Does," R Street Institute, June 2021. https://www.rstreet.org/wp-content/uploads/2021/06/RSTREET232.pdf.

terms of technology for years—from artificial intelligence to military-specific technological capabilities.[11]

There are ways to help mitigate and reduce these concerns, even though China's collection and abuse of data will likely never end. A national data privacy and security law, much like the ADPPA from the 117th Congress, is the most logical next step. I will explore its benefits and how it could address the present data collection crisis.

Acting on privacy legislation makes America more competitive.

Countries around the world have acted on privacy legislation, a prime example being the European Union's General Data Protection Regulation (GDPR). Even China has privacy laws like the Personal Information Protection Law (PIPL) and the Data Security Law (DSL), which have led to rights for Chinese citizens and placed restrictions and obligations on foreign companies operating in China. Unfortunately, these are more likely to be disingenuous attempts by the Chinese government to appear concerned about privacy and security, and competitive with the world, than genuine efforts to promote privacy. This is especially true given the continuous surveillance abuses in China and lack of security for even Chinese citizens' data.[12]

Nevertheless, the United States still lacks a comprehensive privacy law and is becoming an outlier, especially as a country that leads in trade and is looked to as a norm setter. This has led to companies, both American and global, adopting other frameworks as the default. The lack of a privacy law also does not obligate foreign companies to follow specific privacy or security rules while operating in the United States (with some exceptions like entities in regulated

[11] Matt Gimovsky et al. https://www.rstreet.org/wp-content/uploads/2021/06/RSTREET232.pdf.
[12] Karen Hao and Rachel Liang, "Vast Cache of Chinese Police Files Offered for Sale in Alleged Hack," *The Wall Street Journal*, July 4, 2022. https://www.wsj.com/articles/vast-cache-of-chinese-police-files-offered-for-sale-in-alleged-hack-11656940488?mod=article_inline.

industries). In recommending a national data privacy and security law, the Cyberspace Solarium Commission summarized the risk well, noting that "in the absence of congressional leadership, these competing frameworks threaten to splinter the digital economy, confuse efforts to secure users' personal data, and imperil the ability of American companies to compete globally."[13]

Congress has the opportunity to change this by enacting a comprehensive law and clearly conveying the United States' position. It is critical that Congress do this instead of relying on or permitting overreaching federal agencies to decide data privacy and security policy on their own. For example, in the absence of congressional action, the Federal Trade Commission (FTC) is attempting to decide key policy questions on areas that would have major impacts on the nation and privacy in its vast 95 question advanced notice of proposed rulemaking (ANPR).[14]

Data privacy and security legislation provisions can help address privacy and security threats.

Many aspects of the ADPPA would help mitigate data privacy and security threats, but I will highlight several benefits for consideration in any future comprehensive privacy law.

Benefit of data minimization.

Data has many beneficial uses and is foundational to technologies that fuel our economy. However, over-collection of data, especially sensitive data, is not uncommon. This data can easily be misused and/or fall into adversarial control like the CCP. The ADPPA included data

[13] *CSC Final Report*, U.S. Cyberspace Solarium Commission, March 2020. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.
[14] "Comments of the R Street Institute in Response to the Advanced Notice of Proposed Rulemaking," Docket No. R111004, Oct. 12, 2022. https://www.rstreet.org/wp-content/uploads/2022/10/R-Street-Institute-Comments-on-FTCs-ANPR-on-Commercial-Surveillance-and-Data-Security.pdf.

minimization principles, which means data should only be collected to the extent it is necessary or proportionate to provide a product or service, or for a defined permissible purpose. In addition to the value this adds to Americans individually in terms of privacy, it helps reduce the amount of data collected and available in the first place.

There will still be bad actors ignoring this principle, but that is where effective enforcement comes in. Likewise, there will still be entities that pull together publicly available data for malicious purposes, steal data or even purchase it. But steps to minimize it in the first place are beneficial.

Benefit of privacy policies.

An affirmative requirement for privacy policies to alert individuals if their data is transferred or stored in the People's Republic of China, Russia, Iran or North Korea is key. This allows Americans to not only know if this practice is happening, but to make an informed choice about whether they want to engage in the transaction if the data is going to one of those countries. It also promotes transparency by companies, which could even result in a given data transfer not occurring to avoid skepticism from customers.

Benefit of establishing security standards.

Comprehensive legislation should set baseline standards around administrative, technical and physical data security practices to protect data from unauthorized access and acquisition. This provision is essential to ensuring that collected data has safeguards to protect against unauthorized access, whether it be a cyber criminal or nation-state. Equally as important, security provisions should not treat all companies the same, because not all security needs are the same. Practices

should vary based on different factors like entity size, type of data, and cost and availability of tools, among others. Entity size should not always determine requirements, because we have seen small data brokers engage in some of the worst data practices, but it is a factor. Overall, you cannot have privacy without adequate security.

Benefit of strong preemption.

In light of existing state data privacy laws, solving preemption continues to be a roadblock preventing consensus on a federal law. Without a uniform standard across the United States, we would not have a united approach in addressing both privacy and security concerns. The same is true if we do not have a national law at all and states continue to enact laws on an ad hoc basis. For example, one state could require provisions about securing data, but another state might require something completely contradictory or have weaker protections. A citizen's data in one state should not be any less protected than in another. Congress taking the lead on legislation and creating one standard allows for threats from adversaries and bad actors to be dealt with consistently.

Data privacy and security legislation has broader implications.

TikTok has continued to raise concerns on a bipartisan basis. Notably, concerns that user data could be accessed in China and that the platform could be used to spread pro-China propaganda. [15] There are many options for dealing with this, including potential resolution through

[15] Cecilia Kang, "ByteDance Inquiry Finds Employees Obtained User Data of 2 Journalists," *The New York Times*, Dec. 22, 2022. https://www.nytimes.com/2022/12/22/technology/byte-dance-tik-tok-internal-investigation.html#:~:text=%E2%80%9CThis%20new%20development%20reinforces%20serious,Warner%20said.

the Committee on Foreign Investment in the United States (CFIUS) through what is known as "Project Texas," partial bans at the federal and state levels, and a full ban.

Regardless of the path chosen, it is only a partial solution. I say this for two reasons. First, TikTok is just one application from one country. Not only are there risks from other adversarial countries, there are also other current and future applications that will pose risks. Taking a more holistic approach is the key to avoiding potential blind spots. This could entail considering action and review directed at multiple countries and products like some states have proposed in standalone executive orders and directives, including New Jersey.[16] Second, there are many software and hardware products that pose risks like connected devices. For example, there are reports of baby cameras spying on children, electronic locks being remotely opened and robot vacuum cleaners recording people in the bathroom. This has led to some calls for baseline standards and even labels for Internet of Things (IoT) devices, which reflects the National Security Council's current efforts.[17]

While a federal data privacy and security law might not be the full solution, it would serve as a way to help reduce what information can be collected, who it is shared with, require a degree of security, and provide for enforcement should it be violated. Failing to act on federal data privacy and security legislation would ignore the broader risks posed by data and leave threats from China and other malicious actors unmitigated.

[16] Office of Homeland Security and Preparedness, "Joint Circular," State of New Jersey, Jan. 9, 2023. https://nj.gov/infobank/circular/23-01-NJCCIC-OIT-DPP.pdf.
[17] Brandon Pugh, "Is an "energy star label for cyber" the solution to IoT device security and privacy?," R Street Institute, Oct. 21, 2022. https://www.rstreet.org/2022/10/21/is-an-energy-star-label-for-cyber-the-solution-to-iot-device-security-and-privacy.

Conclusion

The United States may lag behind other countries by not having a comprehensive federal data privacy and security law, but the 118th Congress has the opportunity to chart a path forward. This would result in strong benefits to consumers, industry and security. Given competition concerns, increasing threats from adversarial nations and malicious actors, this is more urgent than ever.

Thank you to the Subcommittee on Innovation, Data, and Commerce for holding this hearing. If I can be of any assistance to members of the Committee, please feel free to contact me or my colleagues at the R Street Institute.