Free markets. Real solutions.

R STREET POLICY STUDY NO. 232
June 2021

CONGRESS NEEDS TO START CARING ABOUT OUR PRIVACY AS MUCH AS CHINA DOES

By Matt Gimovsky, Harry Krejsa and Cory Simpson

Editor: Tatyana Bolton

CONTENTS

EXECUTIVE SUMMARY

As much as 90 percent of the world's data was created in the last two years alone.[1] Since then, developments like cheap data storage, rapidly-maturing artificial intelligence and machine learning have accelerated humankind's ability to derive value from this vast new data pool. As a result, our ability to generate, collect, analyze and monetize data is surpassing our ability to consider the consequences such advances hold for our economy, privacy or even national security. The policy implications regarding these changes are profound.[2]

Domestic life is now overwhelmingly conducted online and the data generated by virtue of this activity is a source of great innovation, as the COVID-19 pandemic has laid bare. We are simultaneously blessed with, reliant on and increasingly vulnerable to the complex variables of digital interconnection. Even before the pandemic, it was clear that the expansive digital connectivity we enjoy comes with increasing risks—particularly that of the loss of data security and privacy.

The consequences of data loss now reach far beyond web page defacement. Increasingly, stolen data is becoming a means of harming U.S. national interests via the theft of intellectual property, interference with our elections and financial and reputational loss. In the face of these clear and dynamic threats, the United States must act on data security and privacy legislation. Americans are broadly concerned about securing their data but believe themselves powerless to do anything.[3] Because consumer data now connects national security and consumer protection so decisively, Congress must act to fulfill its constitutional responsibility not only to regulate interstate commerce, but also to provide for the common defense.

Our adversaries have repeatedly demonstrated a willingness to steal our data and commit resources or incur risks to push their visions of a less-secure, less-private, more malleable

Note: The opinions and assertions expressed herein are those of the authors and do not necessarily reflect the official policy or position of the Department of Defense or any other employer.

1. Jacquelyn Bulao, "How Much Data is Created Every Day in 2020," TechJury, May 18, 2021. https://techjury.net/blog/how-much-data-is-created-every-day; The Software Alliance, "What's the Big Deal with Data?", BSA, 2015. https://data.bsa.org.

2. Marc Groman, "As Technology Advances, What Will Happen with Online Privacy," *Forbes*, Jan. 15, 2019. https://www.forbes.com/sites/quora/2019/01/15/as-technology-advances-what-will-happen-with-online-privacy.

3. See, e.g., 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; Rafi Goldberg, "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities," National Telecommunications and Information Administration Blog, May 13, 2016. https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

and more controllable internet onto the world.[4] Congress must demonstrate a similar pragmatism, but one rooted in American values. If the internet is to remain open and interoperable—if it is to be used as a medium over which information freely flows uncensored by government—then Congress must act to ensure the digital realization of our American values.

The 117th Congress's predecessors have fortunately already poured the foundation for strong data security and privacy. The last questions standing in the way of consensus are significant, but imminently surmountable. Lawmakers should keep in mind that their task is not to agree on and then create a utopian ideal for data handling, but rather to establish a strong federal floor for data security and privacy. This robust federal floor will not only protect everyday Americans from data theft and exposure, but will also bring coherence to interstate commerce, improve the global digital interoperability of American businesses, shore up our defenses against cyber espionage and attack, and, critically, demonstrate to our allies and our adversaries alike that American values are not 20th century anachronisms, but are here to stay.

Such a law sounds like a tall order—but consensus is closer than it appears.

INTRODUCTION

After a nearly three-decade hiatus, a near-peer competitor is again challenging the United States' interests and values on the world stage.[5] That competitor, China, is unlikely to provoke a Soviet-style Cold War, but instead presents a long-term strategic challenge altogether more complex and comprehensive than the challenges presented by Moscow. While the Soviet Union waged its competition with the United States through a series of acute crises—such as nuclear brinkmanship and proxy conflicts—the economic foundation required to fully make good on its posturing was absent. In contrast, China's large, growing economy affords it a level of domestic dynamism, international influence and strategic endurance that make it a bona fide competitor. Putin's Russia, for all its considerable and demonstrated ability to harm the United States, can menace, harass and threaten but not supplant the United States as a leading superpower. If Russia is a hurricane—fast, loud and immediately disruptive—then China is climate change as it slowly but inexorably imperils our core interests.[6]

Like present day Russia and the Soviet Union before it, China aims to avoid a direct military confrontation with the United States and instead seeks indirect methods to achieve its goals. One of those strategies is the opportunistic blunting of our non-military advantages.[7] Beijing is less interested than Moscow was in nuclear game playing and damaging proxy wars, but it is already matching or exceeding the Soviet Union's efforts to jockey for economic, diplomatic and other forms of non-military influence across the world.

The need to pair military strength with diverse and varied forms of national power in service of near-peer competition is not unfamiliar ground for the United States. Forged by historical conflict and honed from challenger to challenger, the United States has developed the tools necessary to succeed in competitions that spill off the traditional battlefield. The overwhelmingly digital nature of our rivalry with China means that our digital tools must be updated, along with our strategies, for the current generation's competition.[8] It is clear that the weapons of this new great power competition and the sources of strength that China will seek to subvert are largely data and digital connectivity driven. In addition to data's increasing importance to military tools, it is likewise becoming central to economic projections of the United States' power and influence across the globe. The economy of tomorrow and the values that underpin it could be more important to our national security and global influence than any aircraft carrier or fighter jet.

By market capitalization, 57 out of 100 of the world's largest companies are owned and operated from the United States.[9] American artists help define music, literature and film the world over. Technologies that steer the global economy often build on American education and innovation. The soft power that these advantages confer upon the United States are force multipliers.[10] They win us allies and partners and they win us trade, travel, goodwill and trust, which are far more

4. See, e.g., Sai Ping, "The Chinese Internet—A View from the Inside," Telstra, October 2019. https://pc.nanog.org/static/published/meetings/NANOG77/2067/20191029_Sung_The_Chinese_Internet_v1.pdf; Lily Hay Newman, "Russian Takes a Big Step Toward Internet Isolation," *Wired*, Jan. 5, 2020. https://www.wired.com/story/russia-internet-control-disconnect-censorship.

5. U.S. House Committee on Armed Services, *Future of Defense Task Force Report* 2020, U.S. House of Representatives, Sept. 23, 2020. https://armedservices.house.gov/2020/9/future-of-defense-task-force-releases-final-report.

6. Jean-Baptiste Jeangène Vilmer and Paul Charon, "Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare," *War on the Rocks*, Jan. 21, 2020. https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare.

7. See, e.g., David Shambaugh, "China's Soft-Power Push: The Search for Respect," *Foreign Affairs* 94:4 (July/Aug. 2015), pp. 99-107. https://www.foreignaffairs.com/articles/china/2015-06-16/chinas-soft-power-push; Mingjiang Li, ed., *Soft Power: China's Emerging Strategy in International Politics* (Lexington Books, 2009).

8. John Aquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, (RAND, 1997), pp. 405-34. https://www.rand.org/pubs/monograph_reports/MR880.html.

9. "Biggest Companies in the World by Market Capitalization 2020," Statista, Dec. 1, 2020. https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization.

10. See, e.g., Joseph S. Nye, *Bound To Lead: The Changing Nature Of American Power* (Basic Books, 1990); Joseph S. Nye, "The Information Revolution and Soft Power," *Current History* 113:759, pp. 19-22. https://dash.harvard.edu/handle/1/11738398.

valuable than military hardware over the long term as the world's economies continue to blur together in cyberspace. China, our most likely rival for commercial and cultural influence, struggles to translate regional economic dominance into a cohesive vision that other countries want to support or are incentivized to follow. Even China's regional neighbors, whose economies are inextricably intertwined with Beijing's, stubbornly hold onto political, cultural and security ties with the United States. The unwillingness of China's geographic neighbors to submit to Chinese influence demonstrates a strategic opportunity for the United States to grow a digital economic and cultural advantage as powerful as the Indo-Pacific military fleet and equal to the power that fleet holds over China. Other nations' reticence to break ties with the United States in favor of adopting a Chinese-aligned worldview is exactly why Beijing seeks to erode U.S. sources of soft power rather than pursue a direct confrontation.

The campaign of erosion has already begun. China's vast efforts at economic espionage are well-known with reports suggesting that American intelligence and military assets were already grievously compromised in recent years as a result of Chinese agencies collecting and leveraging large quantities of data.[11] A former deputy director of the NSA's Threat Operations Center described Chinese cyber operations as "robbing the defense industrial base blind" so that government-linked interests could "form a company that would then put that U.S.-side interest out of business" over and over again.[12] These digital espionage innovations, and the vast transfer of intellectual property and wealth they enable costs the U.S. economy hundreds of billions of dollars and allows Chinese firms to leap forward in competitiveness on the strength of American research and development.[13]

Likewise, China is increasingly able to weaponize personal information to imperil Americans' national security. Former Director of the National Counterintelligence and Security Center, William Evanina, warned *Foreign Policy* that China (via both legal and illegal means) has "vacuumed up the personal data of much of the American population, including data on our health, finances, travel, and other sensitive information."[14] By taking merely the information we generate in our day-to-day lives when applying for jobs, visiting the doctor, traveling on vacation or signing up for direct deposits, China can synthesize vast models. These models are intended to identify intelligence agents, thwart counterintelligence measures and stymie U.S. efforts to cultivate sources of information and influence around the world.[15]

Protecting our data and digital connectivity from becoming a medium for our adversaries' aggression is a daunting task. Fundamental cybersecurity is an enduring challenge even for organizations with ample resources and expertise devoted to it, let alone for consumers relying on basic antivirus software for protection. Instilling a culture of vigilance among both consumers and employees is challenging when taken alongside the multitude of tasks required to secure networks and verify hardware. Too often, overwhelmed employers or individuals leave technical and procedural loopholes open for exploitation by malicious actors. The modern economy's storage, processing, transportation and monetization of data creates additional chances for exploitation. These issues illustrate the importance of establishing security standards and unified legal protections built around an understanding of and appreciation for these unique risks.

It is a blessing that today's great power competition appears more focused on technology and economics than military confrontation, but this knowledge comes with the responsibility to ensure that we are ready for non-military conflict.[16] The sources of American non-military power are our democracy, commercial vitality, cultural dynamism and technological

11. House Armed Forces Service Committee, "Future of Defense Task Force Releases Final Report," Press Release, Sept. 29, 2020. https://armedservices.house.gov/2020/9/future-of-defense-task-force-releases-final-report.

12. Zach Dorfman, "Tech Giants are Giving China a Vital Edge in Espionage," *Foreign Policy*, Dec. 23, 2020. https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies.

13. See, e.g., James Andrew Lewis, "How Much Have the Chinese Actually Taken?" Center for Strategic and International Studies, March 22, 2018. https://www.csis.org/analysis/how-much-have-chinese-actually-taken; Office of Public Affairs, "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," U.S. Dept. of Justice, Dec. 20, 2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

14. See, e.g., Zach Dorfman, "China Used Stolen Data to Expose CIA Operatives in Africa and Europe," *Foreign Policy*, Dec. 21, 2020. https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks; Maria Henriquez, "China Has Stolen the Personal Data of 80% of American Adults," *Security Magazine*, Feb. 2, 2021. https://www.securitymagazine.com/articles/94493-china-has-stolen-the-personal-data-of-80-of-american-adults; Andy Meek, "China has Reportedly Stolen Personal Data From 80% of Americans," *BGR*, Feb. 2, 2021. https://bgr.com/2021/02/02/us-vs-china-hackers-stole-personal-data-80-percent-of-americans.

15. See, e.g., Greg Myre, "China Wants your Data—and may Already Have it," *NPR*, Feb. 24, 2021. https://www.npr.org/2021/02/24/969532277/china-wants-your-data-and-may-already-have-it; Evan Osnos, "The Future of America's Contest with China," *The New Yorker,* Jan. 6, 2020. https://www.newyorker.com/magazine/2020/01/13/the-future-of-americas-contest-with-china; Christopher Balding and Robert Potter, "Chinese Open Source Data Collection, Big Data, And Private Enterprise Work For State Intelligence and Security: The Case of Shenzhen Zhenhua," *SSRN*, November 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3691999; Kristin Shi-Kupher and Marekie Ohlberg, "China's Digital Rise Challenges for Europe," Mercator Institute for China Studies, April 8, 2019. https://merics.org/en/report/chinas-digital-rise; Scott Rosenberg, "The U.S. is Now Playing By China's Internet Rules," *Axios*, April 4, 2020. https://www.axios.com/tiktok-crackdown-us-playing-by-chinas-internet-rules-379bf293-fd24-44af-93af-319c850f6500.html; Paul Mozur, "In Hong Kong, a Proxy Battle Over Internet Freedom Begins," *The New York Times*, Feb. 26, 2021. https://www.nytimes.com/2020/07/07/business/hong-kong-security-law-tech.html; Winston Ma, "China Awakens to Digital Privacy Concerns," East Asia Forum, Sept. 7, 2020. https://www.eastasiaforum.org/2020/09/07/china-awakens-to-digital-privacy-concerns.

16. See, e.g., Robert M. Gates, *Exercise of Power: American Failures, Successes, And A New Path Forward in the Post Cold-War World*, (Knopf, 2020), p. 387-390; Kara Frederick, "Democracy by Design: An Affirmative Response to Illiberal Use of Technology for 2021," Center for a New American Security, Dec. 15, 2020. https://www.cnas.org/publications/reports/democracy-by-design.

prowess. These sources of power are increasingly tied up with our data-driven economy, which creates a target that governments like China's are eager to exploit. Accordingly, we have to treat our data as a national security-critical asset that is the rightful property of millions of individual Americans.[17] The United States needs to do away with entrenched and outmoded conceptions of data security in order to break these cycles of exploitation, to protect Americans' data and to solidify America's competitive advantages. The United States can no longer afford to isolate the implementation of technical security mechanisms and design strategy from privacy measures and legal protection. To move into the future, we must acknowledge that when it comes to our digital lives, privacy is security and security is privacy.

WHY WE NEED ROBUST DATA SECURITY AND PRIVACY

China's strategic decision to collect American consumer data gives that data a national security value that is distinct from other kinds of data generated by industries like domestic insurance, advertising and credit. To match this national security need, Congress must urgently act to replace the existing patchwork of state and federal law with a single federal one. Domestically, legislation needs to prioritize consumer data protection.[18] This protection must be put in place to safeguard the competitiveness of small- and medium-sized businesses, whose need to keep their data secure will often outstrip the costs associated with regulatory compliance in the near term.[19] Internationally, legislators should work to make consumer data more difficult to wrongfully access. Doing so will signal the United States' intention to join democracies globally in rejecting the spread of authoritarianism and repression exemplified by China's Great Firewall.[20]

Only a federal law can comprehensively deliver data protection at the speed required to neutralize current international threats. While a triumph for contemporary lawmaking between cybersecurity and consumer protection, the emergence of state data breach notification laws illustrates that the data security and privacy interests of the nation and its individual citizens are most efficiently pursued at the federal level.

At least 15 years passed between the first state breach notification law and the fiftieth. To this day, although laws exist in all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands, a single standard for initial and subsequent action does not exist.[21] Data breach standards should be part of an integrated approach to national cybersecurity. Proposals, like that from the U.S. Cyberspace Solarium Commission offer an example of the shape that a national data breach notification law could take.[22] However, if a federal breach notification law is developed separately from a data security and privacy law, these issues will remain inadequately addressed and will continue to require urgent and persistent fixes of their own.

Establishing a robust federal minimum for consumer data security would simultaneously meet our adversaries in the competition for data while delivering a consistent level of digital consumer protection to the citizens who seek it.[23] Disparities in standard data protections across state and federal law cede ground to adversaries that actively exploit security weaknesses. Congress must act on its responsibility to protect Americans, a duty that now extends to cover the data Americans create and how that data is collected, stored and leveraged by others.

Strengthening the United States' data security and privacy regime would reach far beyond our national legislature to impact the international community. On paper, a given bill might affect particular persons or apply to businesses engaged in a critical mass of interstate commerce, but the reality of the modern digital economy is that how we choose to regulate and secure consumer data resonates far beyond our shores. How the United States regulates entities that collect, store and safeguard consumer data cannot exist in a vacuum apart from questions of geographic reach

17. See, e.g., Cybersecurity & Infrastructure Security Agency, "Critical Infrastructure Sectors," U.S. Dept. of Homeland Security, Oct. 21, 2020. https://www.cisa.gov/critical-infrastructure-sectors; Dr. Jessica Dawson, "Microtargeting as Information Warfare," *The Cyber Defense Review* 6:1 (2021), pp. 63-67. https://www.jstor.org/stable/26994113?seq=1#metadata_info_tab_contents.

18. See, e.g., Sarah Rippy, "US State Comprehensive Privacy Law Comparison," International Association of Privacy Professionals, March 22, 2021. https://iapp.org/resources/article/state-comparison-table; Andy Green, "Complete Guide to Privacy Laws in the US: Compliance & Regulation," Varonis, March 29, 2020. https://www.varonis.com/blog/us-privacy-laws; "Data Security Laws | State Government," National Conference of State Legislature, Feb. 14, 2020. https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx; Brooke Auxier et al., "Americans and Privacy." https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information; "The New Imperative for Corporate Data Responsibility," KPMG LLP, 2020. https://advisory.kpmg.us/articles/2020/new-imperative-corporate-data-responsibility.html.

19. See, e.g., Jeeyun Sophia Baik, "Data Privacy Against Innovation or Against Discrimination?: The Case of the California Consumer Privacy Act (CCPA)," *Telematics and Informatics* 52, Sept. 1, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3624850; "FCC Releases Small Biz Cyber Planner 2.0m," U.S. Chamber of Commerce, Oct. 18, 2012. https://www.uschamber.com/fcc-releases-small-biz-cyber-planner-20.

20. See, e.g., James Griffiths, "Introduction: Early Warnings," in *The Great Firewall Of China: How to Build and Control an Alternative Version of the Internet* (Zed Books, 2019); Larry Diamond et al., *China's Influence & American Interests: Promoting Constructive Vigilance*, (The Hoover Institution, 2018), pp. 18-19.

21. "2019 Security Breach Legislation," National Conference of State Legislatures, July 26, 2019. http://www.ncsl.org/research/telecommunications-and-information-technology/2019-security-breach-legislation.aspx.

22. "Legislative Proposals," U.S. Cyberspace Solarium Commission, July 2020. https://www.solarium.gov/report/legislative-proposals.

23. Kaitlin Asrow, "The Role of Individuals in the Data Ecosystem: Current Debates and Considerations for Individual Data Protection and Data Rights in the U.S.," Federal Reserve Bank of San Francisco, June 3, 2020. https://www.frbsf.org/banking/publications/fintech-edge/2020/june/role-individuals-data-ecosystem; Peter Swire et al., "Online Privacy and ISPS: ISP Access to Consumer Data is Limited and Often Less Than Access by Others," The Institute for Information Security & Privacy at Georgia Tech, May 5, 2016. https://iisp.gatech.edu/working-paper-online-privacy-and-isps.

and jurisdiction, particularly regarding data localization, portability and authentication. In fact, issues of geographic reach and jurisdiction are made more difficult when federal legislators leave states to resolve complexities that potentially have a national and international impact.[24] Simply put, federal law provides the most holistic solution for balancing varied domestic and international needs.

Conventional jurisdictional boundaries increasingly serve as poor analogs for how data is currently handled. State by State jurisdiction is too lumbering for the speed with which consumers generate data, the ease of that data's movement on a global scale and data's nearly perpetual lifetime.[25] The gathering speed and scale of data creation demonstrates our urgent need for comprehensive security and privacy legislation. As policymakers ponder what measures to take in the pursuit of data security and what level of government might champion them, America's adversaries press forward with a relentless march of digital expansionism, making a play for control over the evolution of digital commerce and shaping how digital battles might unfold for generations to come.

To date, legislative activity around privacy and consumer protection has typically been confined to state level, industry or data type, which is a framework that is diminishing in domestic effectiveness. Likewise, broader international investments in norms of data security and privacy will be slow. If federal law continues to embrace its role as arbiter of coherence, stability and interoperability vertically in sectors like finance and healthcare, but neglecting challenges as diffuse and prolific as the privacy of American data, then it will not be able to meet the nation's modern economic and national security needs.

The establishment of a national standard for the treatment of consumer data outside of the National Institute of Standards and Technology (NIST) is required to address the problem of fostering privacy in domestic e-commerce and of enabling the United States to better police the movement of its adversaries across the digital trade environment. As recent breaches make plain, cyber is the ultimate team sport, with an individual's success rising and falling based on the unity and strength of the digital community.[26] If we remove the burden from individual states by establishing a federal set of security requirements, we ensure higher standards and increase the robustness and consistency of data protection by lifting the baseline across the board.[27] At once, a single standard decreases regulatory burden while increasing the security of each individual consumer's data by ensuring that any given byte receives standardized treatment. This buoys our national defense efforts by denying bad actors easy access to data flows.

While the time to maximize impact is diminishing, enough time remains to pass meaningful data security and privacy legislation in a way that embraces fully American ideals. An effective bill must accept that establishing security standards for consumer data will reverberate across economies at a global level. As such, this legislation must be federal, largely preemptive and swift.[28] Such legislative moves will acknowledge the importance of data to domestic and international economies and reestablish what U.S. democratic values look like and what they can do in cyberspace.[29] If we are to keep the internet open, secure and interoperable, then we must have a national standard for data security.

Data is the Lifeblood of a Modern Economy

Data is emerging as the 21st century's most highly sought-after resource. Like crucial resources before it, data's dramatic spike in supply has been met by equally fervent growth in the tools designed to harness it.[30] As a digital commerce and law expert notes, our daily lives generate so much data that merely saying so nearly collapses under the weight of its own self-evidence.[31]

In fact, consumer grazing of the internet generates a data deluge ample enough to create a second-order boon for corporate processors. Decreasing storage costs increasingly allows companies to reach beyond merely obtaining the data necessary to enable their daily operations and shift toward holding

24. Pete Swire, "The Portability and Other Required Transfers Impact Assessment (PORT-IA) Assessing Competition, Privacy, Cybersecurity, and Other Considerations," *Georgia Tech Scheller College of Business Research Paper* No. 3689171, September 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3689171.

25. Yan Carriere-Swallow and Vikram Haksar, "The Economics and Implications of Data: An Integrated Perspective," *International Monetary Fund Departmental Paper* No. 19/16, Sept. 23, 2019, p. 42. https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596.

26. See, e.g., "SolarWinds Security Advisory," SolarWinds, Jan. 29, 2021. https://www.solarwinds.com/securityadvisory; Priscilla Moriuchi, "The New Cyber Insecurity: Geopolitical and Supply Chain Risks From the Huawei Monoculture," *Recorded Future*, June 10, 2019. https://www.recordedfuture.com/huawei-technology-risks.

27. Travis Brennan et al., "California Sets De Facto National Data Privacy," *Corporate Counsel Business Journal*, July 6, 2019. https://ccbjournal.com/articles/california-sets-de-facto-national-data-privacy-standard.

28. Testimony of Xavier Becerra before the U.S. Senate Committee on Commerce, Science, and Transportation, "Revisiting the need for Data Privacy Legislation," 116th Congress, Sept. 23, 2020. https://www.commerce.senate.gov/services/files/8AF136EE-DE50-4258-98C6-249F5BCECFA4.

29. Audrey Guinchard, "Human Rights in Cyberspace," Society of Legal Scholars Conference 2010, Sept. 15, 2010. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1694483.

30. See, e.g., Mike Smith "Data is the world's new natural resource," IBM, Feb. 12, 2019. https://www.ibm.com/blogs/ibm-anz/data-is-the-worlds-new-natural-resource; Liran Einav and Jonathan D. Levin, "The Data Revolution and Economic Analysis," *National Bureau of Economic Research Working Paper* No. 19035, March 2013. https://www.nber.org/papers/w19035; Omer Tene and Jules Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics," *Northwestern Journal of Technology & International Property* 11:5 (2013). https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip; Stew Magnuson, "U.S. Already 0-1 in Tech War with China," *National Defense*, Nov. 11, 2020. https://www.nationaldefensemagazine.org/articles/2020/11/11/us-already-0-1-in-tech-war-with-china.

31. Daniel J. Grimm, "The Dark Data Quandary," *American University Law Review* 68:3 (2019), pp. 761-821. https://pubmed.ncbi.nlm.nih.gov/30919611.

excess 'dark' tranches of data in abeyance, waiting until such time as they choose to extract the potential energy, value and insights locked within.[32] That sufficient data surplus exists to support this type of virtual savings account illustrates the scale of consumer data's present grandeur. Accompanying market actors and tools have proliferated to embrace data's new identity as a commodity replete with capturable economic value.[33] Whereas data of the past conjures grayscale images of clipboard-clutching scientists brooding across sterile laboratories, data's modern manifestation radiates in every hue of technicolor as a resplendent beacon of wealth for those with the analytical inclination to harness it. Critically, the United States and China are far from the only state actors that see capturing and stockpiling data as a strategic and economic imperative to provide an asymmetric advantage on a future digital battlefield.

Combining the continual creation of data with the speed and dynamism of technological growth yields impressive, if not predictable, results. Seven of the United States' 15 most profitable firms are software or telecommunications companies, and the technology industry as a whole represents more than 10 percent of overall economic output.[34] Not only do data-focused companies like Facebook and Alibaba beat the mean S&P 500 growth rate, but also "[d]ata [itself] is becoming a key measure of whether a company will remain relevant through the digital revolution."[35] The same motivators that once caused gold to be under guard at Fort Knox now require a fresh focus on the security of data. Data is easy for unwanted parties to move, it has both inherent and extrinsic value and it is increasingly indispensable to economic policy rationale.[36] If Jared Diamond could reduce 13 thousand years of human confrontation to guns, germs and steel, this paper suggests the next hundred years will be characterized by the economic imposition of policy values, the control of networked communication and the harvesting of data flows that make digital trade wars rationally preferable to traditional warfare.[37]

PRIVACY IS SECURITY AND SECURITY IS PRIVACY

No little effort goes into proposing legislation that grapples with the questions presented by data's rise to power. Lawmakers and industry advocates gravitate toward styling such proposals after consumer protection measures, hoping familiar frameworks will maximize the likelihood of winning consensus. For instance, focusing on rights similar to those in the consumer credit space makes gaining a conceptual foothold much easier than introducing complex legislation organized around the technical elements required to solve a 10-thousand-piece cybersecurity puzzle.[38] However, a legislative solution that meets the magnitude of these issues must accept the relevant order of operations.

Data security is a critical first step before privacy or consumer protection priorities are legislatively or practically possible. Security of the collection, storage and movement of consumer data logically underpins the development of meaningful privacy rights over consumer data. Making data secure is the prerequisite to vesting privacy rights, if for no other reason than to ensure an individual's right to omit, correct or review any such data. Privacy is almost impossible without a market-wide reasonable expectation of who has rightful access to specific data.

While the majority of individuals may not need the most advanced protections against cyber weaponry from China's intelligence services a typical organization's security posture could use guidance from Congress on both normative values and on a desired security end state. In 2019, 1,473 reported data breaches exposed more than 164 million sensitive records.[39] Among others, one global security firm puts the number of all data breaches at 4.1 billion over the first half of 2019 alone.[40] While the first quarter of 2020 saw a 58 percent decrease in public breach reports year over year, the aggregate number of exposed records boomed to 8.4 billion, a 273 percent jump.[41] According to analysis conducted by one cybersecurity company, quarters 2-4 of 2020 contributed another 13.6 billion exposed records, bringing the worldwide year-end total to 22 billion.[42] Without first addressing the insecurity of 22

32. Ibid, p. 764.

33. Swallow and Haksar, pp. 29-33. https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596.

34. "Fortune 500," Fortune 500, 2020. https://fortune.com/fortune500/2019.

35. Yan Carrière-Swallow and Vikram Haksar. https://blogs.imf.org/2019/09/23/the-economics-of-data; Albert Opher et al., "The Rise of the Data Economy: Driving Value Through Internet of Things Data Monetization," IBM, Feb. 2016, p. 2. https://www.ibm.com/downloads/cas/4JROLDQ7.

36. "New Trade Deals, What Kind?", U.S. Chamber of Commerce, 2021. https://www.uschamber.com/issue-brief/promote-digital-trade-and-the-data-driven-economy.

37. Jared Diamond, *Guns, Germs, And Steel*, (W.W. Norton & Co., 1997).

38. See, e.g., The Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681; Paul Jurcys et al., "My Data, My Terms: A Proposal for Personal Data Use Licenses," *Harvard Journal of Law and Technology* 33:1 (2020). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3555188; Jessica Litman, "Information Privacy/Information Property," *Stanford Law Review* 52:5 (2000). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=218274; S.3300; The Data Protection Act of 2020, 116th Cong. https://www.congress.gov/bill/116th-congress/senate-bill/3300/text.

39. See, e.g., Dan Rafter, "Annual number of data breaches and exposed records in the United States from 2005 to 2020," Statista, 2021. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed; Sasha Romanosky et al., "Empirical Analysis of Data Breach Litigation," *Journal of Empirical Legal Studies* 11:1 (2014), p. 74-104. https://onlinelibrary.wiley.com/doi/abs/10.1111/jels.12035.

40. Norton "2019 data breaches: 4 billion records breached so far," Press Release, 2021. https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html.

41. "2020 Q1 Report: Data Breach Quick View," Risk Based Security, 2020, p. 1. https://pages.riskbasedsecurity.com.

42. Future Technology Staff, "Tenable's Analysis Reveals over 22 billion records exposed in 2020," *Future Tech Mag*, 2021. https://futuretechmag.com/tenables-analysis-reveals-over-22-billion-records-exposed-in-2020.

billion records and their storage systems, attempts to inject concrete privacy rights into the morass will be futile. Only after solidifying the floor of minimum technical requirements necessary to strengthen systemic data security can exercisable, impactful privacy rights move beyond the theoretical to impact mainstream consumer life in a way that provides value to individuals and national defense efforts alike.

PRIVACY AS A VALUE

Privacy now sits comfortably alongside speech and association as a preeminent American right. But, "[f]ew values so foundational to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists."[43] Privacy's inherent ambiguity makes legislating a legal framework complicated, and more so because no blackletter entitlement to 'a right of privacy' exists in the Constitution or Bill of Rights. Although there is also no stand-alone privacy right found in an Article of or Amendment to the Constitution, privacy has arguably grown to assume a position of critical importance to constitutional and judge-made law. Well established as a right unto itself, privacy interests serve increasingly as rationale for the deliberate and intentional expansion in other rights that occur as a by-product of common law.[44] How that came to be in the absence of textual origin bears noting.

At its founding, our nation required few of the privacy safeguards that consumers now call for. Safeguarding Americans against government intrusion was 18th century America's order of the day, but these safeguards could hardly foresee a future fueled by digital data points.[45] Accordingly, the lack of direct provisioning from our founders neither detracts from privacy as a core American value, nor poses a constitutional roadblock to necessary congressional action today. Ours is a common law tradition, and as such, the right to privacy exists by virtue of a historical march through the English countryside, across the Atlantic, and over the 1000 or so feet that separate the Capitol Building from the Supreme Court.[46] As applied to privacy, common law processes worked in earnest toward the end of the 19th century.

Samuel Warren and Louis Brandeis recalibrated the common law path in their 1890 law review article "The Right to Privacy," leading it away from what were essentially colonial privacy values and refocusing on the personal rights that we associate with the term today.[47] Their foundational work set the cornerstones of modern privacy rights, emphasized the need to protect them and established four tort mechanisms for doing so: intrusion upon seclusion, public disclosure of private facts, reasonably offensive false light and appropriation.[48] In the spirit of Warren and Brandeis, privacy law and policy extended beyond a fixation on governmental overreach as underscored by the First and Third Amendments. Privacy now means the right to keep classes of thought, belief and behavior sacrosanct not only against one's government but also from the general citizenry.[49]

An adjunct professor at the University of Pittsburgh School of Law, pointed the way toward reconciling both past and present tension in how privacy rights ebb and flow with American culture without a direct constitutional mandate. On the centennial anniversary of "The Right to Privacy" the professor observed:

> [t]he key to understanding legal privacy as it has developed over 100 years of American life . . . is to understand that its meaning is heavily driven by the events of history. What constitutes an engine of privacy in the year 1890, is not necessarily the same thing which formulates a societal notion of privacy in the United States in 1939, or 1968 or 1973. Rather, like a strawberry geranium—saxifraga sarmentosa—which creeps and sprouts new shoots at unexpected intervals throughout its lifetime, privacy in the United States has led a similar vine-like existence, creating a variety of different offshoots depending upon the particular climate of American life.[50]

43. Alan F. Westin, *Privacy And Freedom* (Atheneum, 1967), p. 17.

44. See, e.g., Robert G. Dixon Jr., "The Griswold Penumbra: Constitutional Charter for an Expanded Law of Privacy?" *Michigan Law Review* 64:2 (1965), pp. 197-218. https://repository.law.umich.edu/cgi/viewcontent.cgi?article=5461&context=mlr; R. H. Clark, "Constitutional Sources of the Penumbral Right to Privacy," *Villanova Law Review* 19:6 (1974), pp. 833-34. https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=2046&context=vlr.

45. See, e.g., David H. Flaherty, *Privacy in New Colonial England 1630-1776*, (University Press of Virginia, 1972); Daniel J. Solove, A Brief History of Information Privacy Law, in *Proskauer on Privacy* PLI §1-4 (2006). https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications; "History of Privacy Timeline," University of Michigan, 2021. https://safecomputing.umich.edu/privacy/history-of-privacy-timeline.

46. See, e.g., David A. Strauss, "Common Law Constitutional Interpretation," *University of Chicago Law Review* 63:3 (1996), pp. 877-85. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2999&context=journal_articles; Jim Harper, "Remember the Common Law," *Cato Policy Report* XXXVIII:2, (March/April 2016). https://www.cato.org/policy-report/march/april-2016/remember-common-law.

47. See, e.g., Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 6:5 (1890), p. 193. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf; Solove, https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications.

48. See, e.g., Danielle Keats Citron, "Mainstreaming Privacy Torts," *California Law Review* 98:6 (2010), p. 1805. https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1931&context=fac_pubs; Patricia Sanchez Abril, "Recasting Privacy Torts in a Spaceless World," *Harvard Journal of Law and Technology* 21:1 (2007), pp. 2-47. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1392312.

49. Brief of Scholars of the History and Original Meaning of the Fourth Amendment as *Amici Curiae* in Support of Petitioner in the Matter of *Carpenter v. US*, No. 16-402, 138 S. Ct. 2206 (2018) *Southwestern Law School Research Paper* No. 2017-10. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3028875.

50. Ken Gormley, "One Hundred Years of Privacy," *Wisconsin Law Review* 1992:5 (1992), p. 1335. https://heinonline.org/HOL/LandingPage?handle=hein.journals/wlr1992&div=57&id=&page=; Contra William M. Beaney, "The Right to Privacy and American Law," *Law and Contemporary Problems* 31 (1966), p. 253.

This vine-like existence of legal privacy manifests in the penumbral rights identified by Justice Douglas in *Griswold v. Connecticut*.[51] Over the last 100 years, various iterations of privacy concepts and policy values powered the reiteration of the notion that one's home is their castle, and recognized an "individual interest in avoiding disclosure of personal matters."[52] The primary fixture of privacy's expansion into the electronic universe facilitated by internet connectivity, "informational privacy," emanates from an individual interest in avoiding these types of disclosures.[53]

The difficult work of transferring legal traditions around privacy rights from the physical bounds of the homestead to the digitally connected world is unlikely to slow anytime soon.[54] As the number of people and devices connected to the internet grows, so will the call for privacy rights across the digital space. Current laws will not be able to keep pace with accelerating digital traffic. A federal law would enable the United States' full economic, technologic and cultural strength to manage increased domestic data needs and wage a counteroffensive against Beijing's direct efforts to shape global norms around data handling to their preferred values.

Above, this paper addressed why we can no longer wait for a national data security and privacy bill. Below, the conversation turns to the practical matter of implementation, some of the challenges posed by new legislation and an assessment of the significant work already undertaken. The following section concludes that stripping away the technical aspects of data security from questions of governance eases the way forward and contextualizes the commonplace procedural issues that are part of every federal law standing between where we are today and where we need to be.

BIFURCATING TECHNOLOGY AND ENFORCEMENT IN CONGRESS

In 1965, Gordon Moore, then Director of Research and Development at Fairchild Semiconductor, first observed the pattern for which his name is now commonly known.[55] Moore recognized that the number of semiconductors per integrated circuit, and thus computing power, grew predictably. Based on that observation, "Moore's law" predicted that the power of computer processing could reasonably be expected to double every 18 months or so. While that specific trend stalled in the mid-2000s with an engineering shift to multiple core processors, not only did Moore's law essentially hold true over the interceding 50 years, but it continues to retain relevance as epitomizing the technology sector's brisk rate of change.[56] Today, Moore's law connotes technology's preeminent character trait: speed. Whether pertaining to software, hardware, exploitation, tactics, techniques or procedures, the technological landscape evolves rapidly. By comparison, the government's ability to track, analyze and respond to new technological advances lags.

The disparate top speeds of governance and technology make for a legislative challenge. Happily, for data security and privacy, the good news is two-fold: first, there exists widespread agreement on the technological mechanisms for securing consumer data and second, Congress is well equipped to design an impactful statute primed for enforcement by a preexisting set of expert practitioners.[57] Still, negotiating the nation's first comprehensive data security and privacy bill will require some massaging around the edges of delegation, enforcement authority and the other as-present sticking points. However, considering technical security and legislative procedure separately should allow our elected officials to focus their energies on resolving legislative roadblocks with confidence. In doing so, the technical measures necessary to drive their policy vision will be completely handled through delegation of rulemaking authority and administrative law.

While privacy over data cannot exist without first making data secure against interception and related harms, unfamiliarity with the nuances of end-to-end encryption or prime number cryptography should not prevent voting this necessary bill into law. Moreover, a new law should legislate aims and goals, not prescribe specific security solutions. Any lingering hesitation over how security standards are put into practice or over the speed of technological innovation must be overcome by the urgent national security need to better secure consumer data. Bifurcating the dialogue around technical security from the legislative expertise of Congress will help foster legislative action by removing some of the apprehension to act in this technically complex, dynamic space.[58]

51. *Estelle T. Griswold et al. v. State of Connecticut.* 381 U.S. 479, 483 (1965). https://www.law.cornell.edu/supremecourt/text/381/479.

52. *Robert P. Whalen, v. Richard Roe*, et al. 429 U.S. 589, 598-600 and 24-25 (1977). https://www.law.cornell.edu/supremecourt/text/429/589.

53. *National Aeronautics and Space Administration et al. v. Nelson* et al. 562 U.S. 134, 159 (2011). https://www.law.cornell.edu/supct/html/09-530.ZS.html.

54. See, e.g., *Olmstead et al. v. United States. Green et al. v. Same McInnis v. Same* 277 U.S. 438 (1928); *Charles Katz v. United States*. 389 U.S. 347 (1967); *Michael Lee Smith v. State of Maryland*, 442 U.S. 735 (1979); United States v. Mitchell Miller, 425 U.S. 435 (1976); *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540 (2016); *Manuel Lujian, Jr., Secretary of the Interior, Petitioner v. Defenders of Wildlife*, et al. 504 U.S. 555 (1992).

55. Christopher S. Yoo, "Moore's Law, Metcalfe's Law, and the Theory of Optimal Interoperability," *Colorado Technology Law Journal* 14 (2015), pp. 87-90. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2809676.

56. Neil Thompson, "The Economic Impact of Moore's Law: Evidence from when it Faltered," *SSRN* (2017). https://ssrn.com/abstract=2899115.

57. See, e.g., Richard M. Thompson II and Chris Jaikaran, *Encryption Selected Legal Issues*, Congressional Research Service, March 3, 2016. https://fas.org/sgp/crs/misc/R44407.pdf; Testimony of William Kovacic, U.S. Senate Committee on Commerce, Science, and Transportation, "The Redesign of the U.S. Privacy Policy Institutional Framework," 116th Congress, Sept. 23, 2020, p. 18. https://www.commerce.senate.gov/services/files/8E9CAB53-A529-47CA-9A5B-E59421A29E7D.

58. Daniel J. Solove and Danielle Keats Citron, "Risk and Anxiety: A Theory of Data-Breach Harms," *Texas Law Review,* 96:4 (2018). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885638.

No Special Treatment

Congress should treat a bill to address data security and privacy as it has treated so many others—by legislating a framework and intent while leaving implementation to administrative agencies. We do not require our members of Congress to organically cultivate singular expertise on each complex topic to legislate on those subjects. Within delegation exists an axiom paramount to the modern administration of a federal government, which is that Congress need not assume the twin roles of both drafter and implementer in all cases and may delegate those implementation duties to administrative agencies. While the constitutionality of administrative law fractures the academic community, the notion that administrative agencies are expert in both the statutes they administer and the fields in which they make rules enjoys far greater consensus.[59]

The practical benefits of delegation are considerable. Primarily, it relieves Congress of the need to personally possess the technical mastery required to design discreet enforcement mechanisms before passing laws that frame them. This will imbue the overall system with the speed and agility that may otherwise be lacking. A legislative body that requires strict subject matter mastery prior to action will lag behind emerging markets, threats, technical and social paradigm shifts, and will move at a speed that is inadequate to meet the needs of those they represent. Administrative agencies exist, in part, as a way to help Congress mitigate those potential vulnerabilities by giving it a means to proceed in the face of legislating complex and technical issues. Leaving the balance of execution to delegated administrators addresses the problems germane to legislating in areas that are highly technical and rapidly evolving.

Importantly, delegation does not condone or even contemplate the constitutional permissibility of enabling legislation so broad as to completely vest legislative power outside of Congress.[60] However, Congress can and should leverage the full measure of expertise at its disposal throughout the legislative lifecycle. Sourcing industry input, soliciting expert testimony and drafting committee reports enables Congress to collect evidence and consolidate drafting efforts ahead of a measure becoming law. Once a measure does become law, the delegation of enforcement and of rulemaking authority may foster additional speed, agility and the immediate ability to deploy a technically skilled workforce. Likewise, administrative regulation helps offset some of the disparity between the rate of change in technology and legislative rollout of law meant to keep pace.

The Nine Sources of Material

Before the 117th Congress lies a wealth of industry input, scholarship, testimony and research, all of which can guide it toward passing the nation's first comprehensive data security and privacy law.[61] The herculean efforts of its predecessors primes this Congress as it readies itself for action with the option to leverage content from at least nine separate proposals in its quest to strike the delicate cross-aisle balance now required. Anything crafted will directly address the battle with near-peer adversaries over core conceptions of the Internet, and will confront the economic battlespace of tomorrow: "[C]hange is now on America's doorstep."[62]

At Congress's proverbial fingertips lie five consumer privacy bills, three discussion drafts and the Cyberspace Solarium Commission's legislative proposal. They would not be first to load these documents into a supercollider with the hope that fiercely mashing them all together may reveal some greater elemental truths. The Congressional Research Service synthesized six of the proposals in a sidebar dated April 3, 2020. Before that, it compiled an overview spanning seventy-nine pages ranging from the common law antecedents of privacy law to the relevant industry and sector specific laws protecting particular classes of data trading in narrowly defined spaces.[63] This paper certainly throws a hat into the ring of analysis by picking out certain details and critical themes. However, here, the intent is to emphasize how close consensus could actually be, and how that consensus should be driven by the clear benefits of success and by the menacing consequences of failure.

59. See, e.g., Jerry L. Mashaw, "Federal Administration and Administrative Law in the Gilded Age," *Yale Law Journal* 119 (2010), p. 1362; Lawrence M. Friedman, *A History of American Law* (Touchstone, 1985) p. 439.

60. See, e.g., Philip Hamburger, *Is Administrative Law Unlawful?* (University of Chicago Press, 2014); Christopher J. Walker, "Inside Agency Statutory Interpretation," *Stanford Law Review* 67 (2015), p. 999; *A.L.A. Schechter Poultry Corp. v. United States*, 295 U.S. 495, 529-30 (1935); *City of Arlington v. F.C.C.*, 569 U.S. 290, 305 n.4 (2013); John *M. Mistretta, Petitioner, v. United States United States*, *Petitioner, v. John M. Mistretta*, 488 U.S. 361, 417 (1989) (Scalia, J., dissenting); Christopher J. Walker, "Legislating in the Shadows," *University of Pennsylvania Law Review* 165 (2017), p. 1378.

61. Testimony of William Kovacic, U.S. Senate Committee on Commerce, Science, and Transportation, "The Redesign of the U.S. Privacy Policy Institutional Framework," 116th Congress, Sept. 23, 2020, p. 18. https://www.commerce.senate.gov/services/files/8E9CAB53-A529-47CA-9A5B-E59421A29E7D.

62. See, e.g., Jonathan M. Gaffney, *Watching the Watchers: A Comparison of Privacy Bills in the 116th Congress*, Congressional Research Service, Legal Sidebar, April 3, 2020. https://crsreports.congress.gov/product/pdf/LSB/LSB10441; Eric A. Fischer, Cybersecurity Legislation in the 113th and 114th Congress, Congressional Research Service, March 1, 2017. https://crsreports.congress.gov/product/pdf/IF/IF10610/2; Robert K. Knake, *Weaponizing Digital Trade: Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity*, (Council on Foreign Relations, 2020), p. 14; Paul M. Schwartz, "Privacy and Democracy in Cyberspace," *Vanderbilt Law Review* 52 (1999), pp. 1607, 1615; Homeland Security Advisory Counsel, "Final Report: Economic Security Subcommittee," Department of Homeland Security, Nov. 2020, p. 10; Patrick Murphy and Erica Borghard, "To Defend Forward, US Cyber Strategy Demands a Cohesive Vision," *The Cyber Defense Review* 15:18 (2020), pp. 15-29. https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2420176/to-defend-forward-us-cyber-strategy-demands-a-cohesive-vision-for-information-o; Woodrow Hartzog and Neil Richards, "Privacy's Constitutional Moment and the Limits of Data Protection," *Boston College Law Review* 61 (2019), p. 1687. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3441502.

63. Stephen Mulligan and Chris Linebaugh, *Data Protection Law: An Overview, Congressional Research Service*, March 25, 2019. https://crsreports.congress.gov/product/pdf/R/R45631.

The remainder of this section loosely maps the components of the various proposals available to Congress while identifying some core commonalities, procedural mechanisms and points of divergence, with the latter two largely overlapping. While not resolved here, these three touch points are likely critical to the success of any future legislation. This section also considers how the European Union's General Data Protection Regulation and California's Consumer Privacy Act (and freshly minted Privacy Rights Act) could inform the political left and right's limits of successful federal legislation.[64] Importantly, while analyzing each proposal yields some insight into the political and legislative forces driving these ideas, the analysis leaves our ultimate conclusion untouched: that Congress has an overarching national security imperative to properly secure consumer data. This must be the rally point around which legislative consensus is founded.

The Proposals

Table 1 to the right highlights a smattering of logistical details extracted from the proposals identified above. Any number of data points could be assembled from the sources; however, for the purposes of the discussion to follow, these headings have emerged as principal.

A CORE OF COMMONALITY

While the above proposals emerge from disparate sources, they share a significant amount of common ground. Each proposal directly tackles the difficult jurisdictional questions posed by the transient nature of consumer data, seeking to enhance consumer safety through meaningful and increased consumer participation. Each of these proposals offer solutions, whether it is the right to better access and portability, the benefit of sharper contours around permissible use, or clear consumer authority over when and how data is disposed of or retained.

To a significant extent, each proposal reflects certain policy values of the party sponsoring it. One can look at a bill with Republican roots and associate it by its treatment of preemption, private rights of action, and primary enforcement authority. The same holds true for bills of Democratic origin; they take party-aligned positions on the same points. Table 1 above illustrates the conflict and discord inherent in those issues better than it does the overarching agreement between the proposals or the ultimate prospects for reconciliation and bill passage. It is tempting to only focus on the divergence rather than confluence of these bills and in doing so reinforce potential bias running along party lines. We must resist the temptation of elevating political entrenchment over embracing commonality not only because the need for this legislation is too all-encompassing, but also because cross-aisle agreement is too close to permit failure now.

There are two good examples of common ground between the competing proposals: the need for a federal standard and company-size governing responsibility.

TABLE I: THE NINE SOURCES OF MATERIAL

Bill No.	Short Title	Preemption	Private Right of Action	Source of Governmental Enforcement
HR. 4978	Online Privacy Act of 2019	Placeholder	Y	Digital Privacy Agency
S. 2968	Consumer Online Privacy Rights Act	N; preempt only in conflict	Y	Federal Trade Commission (FTC); new bureau
S. 3300	Data Protection Act of 2020	N; preempt only in conflict	N	New Agency
S. 3456	Consumer Data Privacy and Security Act of 2020	Y; w/ exception	N	FTC
S. 4626	Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act	Y	N	FTC
CSC	Personal Data Security and Privacy Protection Act of 2020	Y; w/ exception	N	FTC
Discussion	United States Consumer Data Privacy Act of 2019	Y	N	FTC
Discussion	House Energy and Commerce Committee "E&C Draft" of 2019	Placeholder	Placeholder	FTC; new bureau
Discussion	Data Accountability and Transparency Act of 2020	N; preempt only in conflict	Y	New Agency

64. Anupam Chandler, et al., "Catalyzing Privacy Law," *Georgetown Law Faculty Publications and Other Works*, (2019). https://scholarship.law.georgetown.edu/facpub/2190.

In terms of federal standards, the majority of proposals base their approach to jurisdiction on the existing statutes governing interstate—or international—commerce. While they sometimes differ in the extent of preemption, all of the proposals recognize that a world with 50 similar but not identical laws on how to conduct business within each state's boundaries would fuel compliance burdens without delivering countervailing security benefits. Appropriately, all of the proposals appear to be, at a minimum, designed to rule out conflict between state laws and a new federal law.

Alternatively with company-size governing responsibility, the proposals generally distinguish the responsibilities of covered entities based on their size. The proposals use either mean gross revenue or the number of individuals whose data is being processed to determine whether the entity processing American's data is a big fish or a small fry, which allows Congress to hold larger entities to a higher standard through a blend of heightened fiduciary duty, increased reporting obligations and required governance structure. This helps safeguard against the greatest threats to data without unduly burdened smaller entities. Further, given the intangible location of data at any given time, agreement on what constitutes a covered entity and the rights and responsibilities commensurate with its status complicates these designations.

These proposals contain real and occasionally seismic departures from one another. Yet one firm fact remains: they have shared end goals. Each proposal aims to enhance consumer safety by providing the right to meaningfully participate in data generation, draw contours around its permissible use, affect when and how data is disposed of or perpetuated and better secure the entire consumer data enterprise. This shared goal points optimistically to the passage of a federal law. Congress should find the means required to push past the partisan issues preventing forward movement of legislation in this space with a renewed appreciation for and focus on the common goal of delivering increased consumer protection through standardizing data security protocols across the consumer data processing environment.

POINTS TO BE RESOLVED

It is time for Congress to determine how the flashpoints of contention are to be resolved and pass the nation's first comprehensive data security and privacy legislation into law. Although each proposal pursues the same aims, the proposals currently under consideration use different legislative and legal tools to achieve the same results. Much of the division that prevents any one of the proposals from emerging victorious emanates from issues of perspective. Understanding that federal data security and privacy legislation is a pressing national security need, should turn Congressional impasse into Congressional action.

Whether a proposal tackles vesting individual rights over consumer data by proceeding from a broad invocation of values like the Data Protection Act of 2020, or begins more concretely with the need to uniformly set security minimums in the style of the Consumer Data Privacy and Security Act of 2020, we need to come to a resolution. Resolving the underlying confusion should help solidify where each proposal falls on the inclusion of a private right of action. It will also clarify if primary enforcement lies with the FTC and what modicum of state law remains in the aftermath. At baseline, federal legislation serving the dual purpose of protecting consumers and squarely meeting emergent national security threats requires only two things. First, it must establish strong and uniform security benchmarks for all participants in the domestic data market applicable throughout the processing lifecycle.[65] Second, those standards must be enforced by the FTC.

Due to the inherent interconnectedness of cybersecurity, better security in one sector results in better security for all. The web-like topology of the internet is both a strength and a vulnerability.[66] As a result, establishing minimum security standards for entities will have a huge return on value. Imposing a uniform security floor calculated to ensure systems are updated and patched at a known cadence, or that regulated entities have firewalls and encryption standards in place, will create benefits spanning not only that specific organization but also across the American internet ecosystem as a whole.

However, without an agency primed to enforce a uniform security floor, the consistency and predictability created by a federal security standard wins only half the battle. The FTC must take a primary enforcement role and it must receive the reinforcements it deems reasonably necessary for that purpose.[67] Anything less merely papers over the cracks without filling them in by supplanting a tangle of laws with a single one. Further, it would ignore the skills and experience cultivated by the FTC in the more than 15 years that it has enforced the Federal Trade Commission Act in the digital space, and it would expend enormous amounts of time establishing, funding, staffing and unleashing a new agency.

---

65. Dymples Leong and Teo Yi-Ling, "Data Brokers: A Weak Link in National Security," *The Diplomat*, Aug. 21, 2020. https://thediplomat.com/2020/08/data-brokers-a-weak-link-in-national-security.

66. Steve Lohr, "He Created the Web. Now He's Out to Remake the Digital World," *The New York Times*, Jan. 10, 2021. https://www.nytimes.com/2021/01/10/technology/tim-berners-lee-privacy-internet.html; Richard A. Clarke And Robert K. Knake, *Cyber War: The Next Great Threat To National Security And What To Do About It*, (Ecco, 2010), pp. 265.

67. Chris Jay Hoofnagle et al., "The FTC can rise to the primary challenge, but not without help from Congress," The Brookings Institution, Aug. 8, 2019. https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress.

Among the remaining variables there are viable combinations that could accomplish the international policy goal of secure consumer data. Considering these options separately appears to breed disagreement over a private right of action, the scope of preemption and primary enforcement authority. Instead of taking each variable as a stand-alone legal issue warranting its own resolution, we should select a combination of the solutions contained within the source material of the proposals. For example, examining oversight responsibility reveals options to include state attorney generals among the enforcers in a role complementary to the FTC.68 Recognizing the value added by state enforcers makes more than just practical sense, especially given the amount of data, number of regulated entities and volume of affected Americans at play. Recognition of state enforcers signals to the market that oversight will be intelligent and robust rather than delayed by internal dissent over prosecutorial jurisdiction. A compromise that includes state enforcers in addition to federal enforcement lets the American people know that their Congress values the security of their data more than politicking.

Similarly, agreement on a limited private right of action, like that given by California to its residents, could serve as a strong rallying point.[69] While critics of the limitations placed around California's private right of action are correct to say it is leaner than similar rights in other federal statutes, it proves that a compromise is reachable. In light of California's successful inclusion of a private right of action, it is no longer enough to hold up the progress of a federal bill on that issue alone.

A more difficult but similarly solvable issue is whether to partly preempt state law or to step into the entire space. Which relevant state laws will persist subsequent to the federal one is difficult to predict, as many were passed to fill the void in national law. While uniformity and certainty are benefits typically espoused by proponents of preemption, out of necessity, California's Consumer Privacy Act (CCPA) has risen to a de facto standard for industry in its attempt to mitigate the costs incurred by tracking and adhering to various regulations that concern data. Alongside the recent passage of the Privacy Rights Act, consumer protection tools in California are only set to expand. In the absence of Congressional action, individual state laws including some on specific subtopics will leave industry with an all-or-nothing choice to either accept California as a minimum standard or pour additional resources into tracking disparate state requirements.[70] By and large, industry has adopted the former strategy.

Industry response to the Californian position is robust and insightful.[71] At minimum, these lessons ought to be incorporated into the final federal law. If broad preemption is chosen, the standards set by Californian law stand as a reference point that could help ease industry's transition to the new compliance standard. Conversely, if the federal standard falls beneath the Californian one, state law could foreseeably remain in charge, albeit under the banner of Federal Law.

In a similar vein, the European Union's General Data Protection Regulation and the CCPA are cognizant of one another in certain respects.[72] Congress would be right to keep the European and Californian interplay in mind, as well as the evolution with the Court of Justice of the European Union's recent decision to strike down Privacy Shield, i.e., the EU-U.S, personal data transfer mechanism that when complied with permitted companies to freely transfer users' personal data between the European Union and United States.[73] Without Privacy Shield, there is no functional mechanism for U.S. companies to exchange personal data with their European counterparts. If handled with intention, our nation's first data security and privacy legislation presents an opportunity for Congress to address that problem and enable stronger connections between the United States and our longest standing democratic allies in Europe.

CONCLUSION

This paper seeks to reframe the need for data security and privacy legislation to acknowledge a stark reality: Xi Jinping's Chinese Communist Party is placing a high priority on everyday Americans' data and it is past time that Washington do the same. The case for such a law also extends

68. See e.g., SIL 20710, Discussion Draft, the *Data Accountability and Transparency Act of 2020*; Cyberspace Solarium Legislative Proposal; The *Personal Data Security and Privacy Protection Act of 2020* § 9, Enforcement by State Attorneys General; Danielle Keats Citron, "The Privacy Policymaking of State Attorneys General," *Notre Dame Law Review* 747 (2016). https://digitalcommons.law.umaryland.edu/fac_pubs/1595.

69. Dee Pridgen, "The Dynamic Duo of Consumer Protection: State and Private Enforcement of Unfair and Deceptive Trade Practices Laws," *Antitrust Legal Journal* 81:3 (2017); Brian Galle, "Valuing the Right to Sue: An Empirical Examination of Non-profit Agency Costs," *Journal of Law and Economics* 60: 3 (2017). https://www.journals.uchicago.edu/doi/abs/10.1086/694738; *Enforcing Federal Privacy Law--Constitutional Limitations of Private Rights of Action*, Congressional Research Service, Legal Sidebar, May 31, 2019. https://fas.org/sgp/crs/misc/LSB10303.pdf

70. See, e.g., Cynthia Brumfield, "12 New State Privacy and Security Laws Explained: is your Business Ready?", *CSO*, Dec. 28, 2020. https://www.csoonline.com/article/3429608/11-new-state-privacy-and-security-laws-explained-is-your-business-ready.html.

71. See, e.g., Paulius Jurcys and Markus Lampinen, "Principles of Data Privacy in California, Study of Industry Reactions and Comments to the Proposed CCPA Regulations and User-Centric Perspectives," *SSRN*, May-June 2020. https://ssrn.com/abstract=3601948.

72. See, e.g., Jordan M. Blanke, "Protection for "Inferences Drawn:" A Comparison between the General Data Protection Rule and the California Consumer Privacy Act," *Global Privacy Law Review* 1:2 (2020), pp. 81-92. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518164; *California Dreamin' of Privacy Regulation: The California Consumer Privacy Act and Congress*, Congressional Research Service, Legal Sidebar, Nov. 1, 2018. https://fas.org/sgp/crs/misc/LSB10213.pdf; Nicholas F. Palmieri III, "Who Should Regulate Data?: An Analysis of the California Consumer Privacy Act and its Effects on Nationwide Data Protection Laws," Hastings Science & Technology Law Journal 11:1 (2020). https://repository.uchastings.edu/hastings_science_technology_law_journal/vol11/iss1/4.

73. See, e.g, *Court of Justice of the European Union ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems* ("Schrems II") decided July 16, 2020.

beyond the defensive by also promising to be a key enabler of commercial and geopolitical innovation. Providing direction to the marketplace and laying a legislative foundation will allow American companies to more easily interface with the privacy and security regimes of our democratic allies, making interoperability and e-commerce easier with those countries that have already embraced 21st-century data legislation. The United States will also be able to more credibly wield its values as tools of foreign policy having moved beyond extolling them and graduated to committing those values to law.

These economic and political breakthroughs are within grasp. While a federal floor delineating rights and responsibilities of consumer data stakeholders sounds daunting in the abstract, Congress has already achieved 80 percent of the work. Finishing the last 20 percent of such a bill by settling issues of preemption, private right of action and agency enforcement will admittedly be difficult, but there is nothing uniquely divisive about these challenges and lawmakers routinely settle such issues. More difficult is attempting to compete with China without such a law.

ABOUT THE AUTHORS

Matt Gimovsky is a legal advisor in the U.S. Army Reserve and a Senior Principal Subcontracts Specialist at Raytheon Technologies. He works on technology transactions related to the contractual and supply chain components of cybersecurity, including enterprise risk management and tech policy.

Harry Krejsa is a fellow at the Center for a New American Security, served as Deputy Lead for the Cyberspace Solarium Commission's Integration Cell and lectures on defense and technology policy at George Washington University.

Cory Simpson is a managing director in cybersecurity and privacy practice at Ankura, adjunct professor at Clemson University and legal advisor in the U.S. Army Reserve with assignment to U.S. Special Operations Command.