JUNE 2023

Restricting China or Repairing Loopholes:

Washington's Incomplete Efforts to Protect Data

Yilun Zhang
Amanda (Yue) Jin
Alec Caruana

中美研究心 ICAS
Institute for China-America Studies

About ICAS

The Institute for China-America Studies is an independent think tank in Washington D.C. ICAS focuses on the evolving dynamics in the U.S.-China relationship to promote greater collaboration and mutual understanding through sincere exchanges of fresh ideas, objective policy-oriented research, and fair assessments of this critical bilateral relationship. Our research covers China-U.S. strategic relations, maritime security, economics, trade and technology relations, climate change and environment policy, global governance, and other issues central to the bilateral relationship.

Ultimately, we aim to provide a window into the worldviews of both the United States and China, and thereby serve as a vehicle to promote greater understanding between these two countries and societies.

ICAS is a 501(c)3 nonprofit organization.

ICAS takes no institutional positions on policy issues. The views expressed in this document are those of the author(s) alone.

Cover Image: Senate Select Committee on Intelligence Mark Warner (D-VA) talks to reporters while introducing the Restrict Act at the U.S. Capitol on March 07, 2023 in Washington, DC. In reaction to software built in countries hostile to the United States, including China's TikTok, the new legislation would allow the Commerce Department to take action on suspected foreign spying risks in artificial intelligence, fintech, quantum computing and e-commerce. (Photo by Chip Somodevilla/Getty Images)

Institute for China-America Studies
1919 M St. NW Suite 310
Washington, DC 20036
202 968-0595 | www.chinaus-icas.org

Acknowledgements

This report would not have been possible without the support of the ICAS Trade n' Technology Program and the program's past analytical works. We would like to express our deepest gratitude to Sourabh Gupta, Jessica Martin and the rest of the ICAS team for their generous support throughout the making of this endeavor.

– YZ, AJ & AC

About the Authors

Yilun Zhang is a Research Associate and Administrative Officer at the Institute for China-America Studies. He is also the manager of the ICAS Trade'n Technology Program. His key area of research pertains to U.S.-China relations, trade and technology, security and the international relations in the Indo-Pacific region. His areas of specialization include: analysis of the U.S.-China strategic competition on security and trade and technology; analysis of major power relationships in East Asia (China-Japan-South Korea-U.S.) and trending issues in the Indo-Pacific region; analysis on the security dynamics in East Asia; and geospatial analysis of the security dynamics in the Indo-Pacific and Arctic region. He holds a master's degree in international relations with a concentration on international political economy from the Paul Nitze School of Advanced International Studies, Johns Hopkins University.

Amanda (Yue) Jin is a Part-time Research Assistant at the Institute for China-America Studies and a member of the ICAS Trade n' Technology Program team. Her research interests include the U.S.China technology and innovation competition, the governance of data and new technologies, and the international law of the sea. She holds a B.A. in Political Science/International Relations from Carleton College and a J.D. from Harvard Law School. She is currently pursuing a Master's degree in International Relations at the Paul Nitze School of Advanced International Studies, Johns Hopkins University.

Alec Caruana is a Part-time Research Assistant at the Institute for China-America Studies and is a member of the ICAS Maritime Affairs Program and Trade 'n Technology Program teams. His research interests include studying the South China Sea from historical, legal, and security perspectives and analyzing the foreign policy of smaller states in the Indo-Pacific amid increasing great power tensions. He holds a BSc in International Relations and History from the London School of Economics and Political Science where he specialized in cartographic history, American foreign policy, and Chinese involvement in the Global South. He is currently finalizing a joint master's degree in International Affairs taught jointly by Peking University and the LSE.

Contents

I-II Executive Summary

1-2 Introduction

3-6 PART 1 | Before Meta and TikTok:
The "Patchwork of Federal Privacy and Data Laws"

7-13 PART 2 | Big Tech Era:
Free Expansion of America-led Businesses

14-22 PART 3 | Before Meta and TikTok:
When the American Catch-up Turned Hysterical

23-24 Conclusion

- APPENDICES -

Appendix A: Notable Data Privacy Laws in the U.S., 1970s to 2000s

Appendix B: Summary of State-level Data Privacy Laws
(California, Virginia, Colorado, Utah and Connecticut)

Executive Summary

As the United States moves into the third decade of the 21st Century, policymakers and lawmakers have come to realize, and, accordingly, panic about the imminent need to reform the existing data governance regime. However, efforts to patch up, and thereafter, roll out a sophisticated data governance system is troubled by continuous imbalance and, to some extent, skewed prioritization of policy. Washington failed to seek a way out of the pickle that it set for itself: to compete with China and address its challenges while, at the same time, to enact a consistent, long-term systematic data governance structure. Similar to much of the policy-making in recent years, security concerns over threats posed by China have dominated the minds of policymakers and legislators. The efforts to protect data have therefore been distracted and misled dramatically by the, sometimes hysterical, sense of insecurity about China. The work is incomplete and the prospect for completion is becoming increasingly concerning.

The genuine concern over U.S. data governance reform can be traced back to the early days of the tech industry boom. The fact that the United States had adopted a laissez-faire model to inspire its tech industry to expand into 'no man's land' brought both tremendous opportunities for U.S. businesses to trailblaze globally, alongside enormous challenges to regulate this rapidly inflating market. Under such a laissez-faire model, government actions were only responding to imminent needs for top-down intervention instead of building a long-term consistent system. The loopholes therefore lurked and grew as the market continued to evolve and eclipse the old 'patchwork' of reactive policies.

Loopholes and systemic challenges continued to grow into a more serious problem throughout the first decade of the 21st century, which marked a period of globalization and regional economic integration empowered by the global Internet boom. This was also the period when cybersecurity, business data and secrets, and personal privacy became an issue of concern for not just policymakers, lawmakers, and businesses, but also the general public. More focus and questions emerged

on how to better strengthen America's own data governance system. That said, American tech giants continued to thrive during the period when the problem of regulating and managing the Big Techs emerged as a valid and imminent concern for Washington. Despite the growing consensus to 'do something' about the Big Techs, Washington lacks the sophisticated consensus and, therefore, consistent motivation to push out specific and enforceable measures to close the loopholes. The system continues to follow the old trajectory despite the fact that the data practices it intended to govern have entered a new generation.

While the Europeans and the Chinese pushed out their respective systemic, enforceable, top-down, forward-thinking and consistent data governance systems, the United States has continued to struggle at present to push out its own data governance overhaul. The lack of consensus to fix the problem is not the main predicament for Washington anymore. Washington's passion to compete with China and its significant reluctance to wade through the swamp to reform its data governance system produced a distraction from its intended aim to improve the situation in the long run. Short-term, eye-catching policy efforts to address the China data threat have dominated national headlines and the minds of Washington policymakers and legislators. The enormous resources spent on the push for the RESTRICT Act, the efforts to pass the American Data Privacy and Protection Act (ADPPA) and the topical yet fruitless public humiliation of TikTok on Capitol Hill are just a few encapsulations of Washington's big failure to enact concrete, long-term, systemic data governance structure. The work is incomplete. The focus is not on data, but on China.

In order to release itself from its current predicament, Washington should first draw a clearer distinction between the short-term China threats and the long-term need to cement capable and sophisticated data governance structures, and prevent the former from distracting and misleading the latter in future policy discussions. Washington should also work closer with business communities, both domestic and international, to improve its current regulatory measures and increase the pace on its efforts to coordinate with Europe and China on global data governance. Tech businesses are at the forefront of the global digital economy and they will benefit from a better coordinated global data governance system. Washington should make use of business incentives rather than making enemies by categorically shaming Chinese and foreign companies and alienating domestic tech communities.

Introduction

Data is everywhere and everything. Through digitalization and the further expansion of the Internet and other networks, vast amounts of individual and collective information flow through every sector and every realm of our daily lives. The application of data is not just a fancy concept but rather a realistically efficient, reliable and effective tool to refine searches, identify needs, and thereafter, tailor optimized approaches to each of the data users. That being said, data has also proven to be a double-edged blade in this third decade of the 21st century. Without proper governance, data presents grave challenges to national governments, businesses and individual lives at the same time it continues to improve prosperity and connectivity. The introduction of Big Data approaches has helped governments to better manage critical public emergencies such as the COVID-19 pandemic, but it simultaneously poses questions and suspicions that governments might misuse these data to either tighten individual profiling or manipulate the public opinion. The application of Big Data could gradually improve the efficiency of work and the effectiveness of business strategies, but open up the hazards of hacks and leaks. Personal information, if shared and used appropriately through the right channels and under the right supervision, can improve user experience. However, big companies that over-collect user data naturally pose a moral concern if their practices are unregulated.

The question of data gets more complicated when the elements of international politics come into play. Next-generation warfare will be heavily dependent on Big Data and artificial intelligence. Just as the Russia-Ukraine War has raised concerns about information warfare, the protection and usage of data will have significant implications for national security. Big multinational tech companies operating under multiple jurisdictions raise questions about the collection and storage of data, while concerns over the companies' own data security have emerged as they become targeted by criminal activities from no longer one but multiple countries. Personal data collected and used in different countries pose a significant challenge to cross-border privacy protection—namely, how effectively countries can cooperate and coordinate and how and who should lead such progress.

As the world's leading economy, the United States used to be the pioneer and avant-garde of groundbreaking innovation and reform. However, as the world becomes increasingly digitized and interconnected, recent investigations, hearings and insider revelations have shed light into

the outright lack of data governance in the United States. On one hand, the country is facing an increasing number and variety of genuine external threats from state and non-state actors with regard to data security. On the other hand, the rapid expansion of Big Tech companies and the complication of governing or regulating cross-border flows have presented the United States a critical yet difficult task to balance supporting businesses' growth potential with establishing guidelines, principles and guardrails. Moreover, strategic competition with China and the less-mentioned yet ongoing competition with the European Union over standard-making and innovation have left the U.S. little room to resolve its internal differences over the specific practices on data governance. The clock is ticking for the United States to catch up to China and Europe on rulemaking alongside its attempts to to lead Brussels and outcompete Beijing.

To kick-start the U.S. policy discussion during this critical moment, it is important to bear in mind the origins and the fundamental needs behind the establishment of the U.S. data governance system to clarify the essential areas, foreseeable challenges and known opportunities that the United States needs to prepare itself for. Meanwhile, the state of strategic competition with China strengthens yet complicates the need for improving data governance in the United States. In the complicated political and policy environment of today, the policy discussion around data governance risks becoming a huge spaghetti bowl. Unpacking each of these relevant individual issues will be very helpful for policymakers to determine their priorities and thereafter, decide on their policymaking roadmap.

The purpose of this report is to draw a clear distinction between two types of policy considerations and solutions: those that aim to build an American data governance regime of the future, and those that seek gains vis-à-vis trade and technology competition with China. By tracing the history of U.S. data governance, the unresolved concerns of the Big Tech era and the most recent efforts for reform and new measures, the report seeks to clear the air and identify the real issues lurking within the U.S. data governance system. With the existing 'patchwork' national data regime, most of the many loopholes in the U.S. data governance have originated from the lack of a systematic, comprehensive or even ex ante approach to concerns such as data security, privacy and the appropriate regulation of the technology industry. Accordingly, even when talks about China naturally arise when these loopholes run into China-related issues—e.g. a Chinese technology company—the underlying policy issue is often not China-specific. As China-focused investigation, analysis and proposals have prevailed in the policy discussion surrounding U.S. data governance, the efforts to outcompete China often mislead and distract the halfway efforts to push through U.S. data governance reforms.

PART 1

Before Meta and TikTok: The "Patchwork" of Federal Privacy and Data Laws

Ever since American companies began their trailblazing role in the global digital economy, the United States has never developed the tradition to regulate the technology industry—and by extension, data matters—comprehensively. Until the 2010s, a more-or-less laissez-faire approach fueled free innovation, enabled the success of a vibrant technology industry and, at most times, meant that the innovators and industry stakeholders felt the need and obligation to develop effective means of self-governance. Under such a model, the introduction of government action is only considered when emerging challenges expose an imminent need for top-down intervention. Even then, regulatory responses tended to narrowly address only the issue at hand, leading to a growing body of rules and standards that focus on specific sectors or types of data. As researchers and commentators have aptly articulated, the existing U.S. data governance system is best described as a "patchwork" approach to protect data and privacy in select fields and in a non-comprehensive manner.[1]

Data first became an issue of discussion in the 1970s, at the advent of the Information Age. As the collection and processing of mass personal information became a prominent practice, the rising need to ensure minimum protection of these data was at odds with the lack of any governance structure to ensure a bottom line of practice standards. Key to this development was the Supreme Court's decision to offer very limited constitutional protections for an individual's right from the collection and dissemination of their personal information.[2] As protection against government programs or prevailing information collection programs could not be obtained through judicial means, the legislative branch had to step in and bring in regulations to areas of most concern and sensitivity to U.S. citizens.

Focusing on the most imminent data concerns in the 1970s—the impact of credit reports, the usage of children's educational data and the confines of government authority, these early laws were designed to narrowly address the specific problems at hand. [See Appendix A for a list of notable data privacy laws from the 1970s to 2000s.] For example, in 1974, the Privacy Act was introduced to establish a set of basic requirements and guidelines for government agencies

Three of the most popular commercial personal computers in the late 1970s; left to right: PET 2001; Apple II and TRS-80.
(Source: Tim Colegrove; CC BY-SA 4.0)

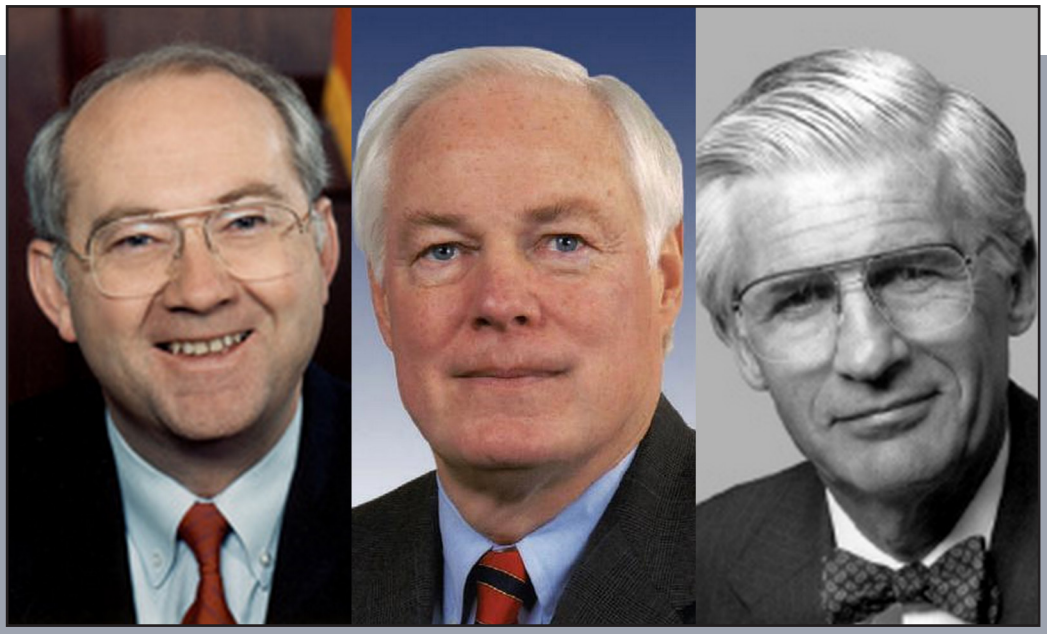
as they collect, maintain, use and disseminate personally identifiable data of individuals in the United States.[3] Although the Privacy Act established a detailed list of "fair information practices" including the individual's right to request their records, the right to correct or update their records and the right to be protected against unwarranted invasion of privacy,[4] these requirements stemmed from the specific obligations that the U.S. government—as opposed to e.g. companies and private organizations—owes to U.S. citizens, while the political necessity of the bill originated from the especially weighty consequences of government misconduct and overreach. Even in the 2020s, the U.S. government widely sees the Privacy Act as one of the requirements for the respective internal regulation of each individual department and agency. As such, these standards and obligations are more closely connected, administratively or politically, to the application of the Freedom of Information Law (i.e. an individual's right to request certain records from the executive branch) than either the constant efforts to ensure whole-of-government data security or the call for a federal framework of data privacy.[5]

Although these earlier laws helped establish precedents and principles that later rulemaking efforts sometimes consulted, regulators seldomly saw the need to establish consistency across the various issue-specific regulatory structures. As the patchwork mentality focused only on addressing imminent challenges that threaten the very fundamentals of society and morality,[1] it was impossible to push for systematic change or reform that could be powerful enough to reshape or encourage a different pattern of data practices across the system. The Gramm-Leach-Bliley Act serves as a typical case. Although highly influential with regard to data practice standards within the financial institution, the Act failed to either build upon prior models or inspire changes beyond the financial sector. Instead, policymakers used much creativity and talents to invent another set of principles and practices that is specifically

1 Examples of these imminent challenges include (a) the risk of cable industry abuse following massive deregulation; (b) the leak of personal information in the public driving license databases; and (c) the protection of sensitive patient health information given the growing popularity of medical insurance and accordingly, the prevalence of massive health information transfer across various institutions. [See Appendix A for a more detailed list.]

tailored to the financial industry. Where preceding laws such as the aforementioned 1974 Privacy Act established an individual's right to obtain and correct their records, and when contemporary 1990s law chose to e.g. prohibit disclosure of sensitive information without express consent or assign relevant agency to establish and impose data privacy standards, [6]the Gramm-Leach-Bliley Act took yet another approach. Under the Act, certain financial institutions are required to provide privacy notice to their customers and provide these customers a "reasonable opportunity" to opt-out when the institutions intend to share their personal data to nonaffiliated third parties.[7]

Although the Gramm-Leach-Bliley Act provides another noteworthy model of data governance, the likes of these regulations did not extend beyond the financial sector until California introduced the right to opt out through the passage of the California Consumer Privacy Act (CCPA) in 2018, while federal application of these rights and obligations beyond the financial sector remains only in legislative proposals and discussions. As each of the regulatory model functions as a one-time solution to one specific problem, none of the data-related laws and provisions have succeeded in establishing a powerful, repeatable, and referenceable precedent that could initiate more systematic legislation or group of legislations that aim to reshape or properly guide the development and practices of the entire technology sector.



The Co-sponsors of the Gramm-Leach-Bliley Act; left to right: Sen. Phil Gramm (R-Texas), Rep. Jim Leach (R-Iowa), and Rep. Thomas J. Bliley, Jr. (R-Virginia). (Source: Adam sk; public domain work)

Even as the Federal Trade Commission (FTC) was charged to enforce a multitude of data privacy related laws and regulations, the Commission has been able to establish consistency across the myriad rules and standards it was told to enforce, let alone providing a systematic framework for data governance. As of 2023, and to cover a few of FTC-enforceable regulations,

a company would be required to follow the aforementioned Gramm-Leach-Bliley notification requirement if it is in the financial sector; post clear online privacy policy, obtain parent consent and reasonably protect children data with regard to certain children's data; promptly notify all customers of data breaches with regard to certain health data; establish reasonable data protection routines with regard to credit reports and commit to the pledges they've made in their privacy policy with regard to consumer privacy.[8] Although the FTC has attempted to improve some clarity through administrative rulings and guidelines,[9] its power mostly lies in sector-specific ex post rulings and guidelines, limited by the bulk of statutes that established the Commission's very authority. Without a comprehensive, on-topic authority granted by the Congress, FTC can do little to disentangle the web of sector-specific patches that has defined U.S. data governance since the 1970s.

Accordingly, the U.S. data laws and regulations have been unable to evolve beyond their original, narrow purposes, let alone address emerging and unanticipated challenges over time. As the leading pioneer in digitalization, globalization and innovation, the United States has seen the need to govern and regulate data across a number of issues even despite its laissez-faire tendency. While these laws and regulations should have helped form guardrails against foreseeable challenges and stimulated changes and best practices across the system, policymakers have chosen to overlook the lessons they could have drawn from the past. Ironically, many of the earlier U.S. data governance practices—such as those seen in the Privacy Act and the Gramm-Leach-Bliley Act—would be later observed in the laws of the European Union and China as they systematically regulate data practices and stimulate their technology industry. In contrast, when bigger changes happen, it is almost impossible for the United States to be well-prepared for the shock.

PART 2

Big Tech Era:
Free Expansion of America-led Businesses

The global Internet boom, empowered by globalization and regional economic integration in the early 21st century, has presented new opportunities together with a host of leveled-up challenges. On one hand, as the avant-garde of the Internet, U.S. big tech companies spread their network to other emerging global markets, specifically Asia. American influence, together with American economic success, peaked in the first decade of the 21st century. However, glories come with a shade of danger. Non-state threats such as Al Qaeda and adversary states such as Russia and North Korea opted for a cyber approach to level their advantage against the U.S. These asymmetric security challenges have gradually challenged the traditional great power-oriented U.S. national security approach. Moreover, despite the temporary downfall during the 2008 financial crisis, new Big Tech companies including Google, Apple and Facebook (now Meta) contributed to global recovery, and thereafter, a new wave of prosperity led by American-made technology and the Internet. Businesses are now done in a different way, and a new type of industry is leading the economic growth. Technology and the Internet surpassed housing, real estate and energy to become the new 'Gold Rush.' Nevertheless, these American pioneer businesses run into cross-border problems as they find themselves struggling between expanding into emerging markets with high growth potential, especially China, and the need to establish a universally accepted consensus over cross-border data and business practices. The explosive introduction of social networks has changed the way of life of every single American. Americans are now able to connect with and learn about people from the other side of the planet in a split second. However, the open nature of social media yields ground to malign usage of individual information, online stalking,harassment and public abuses with more serious consequences. New challenges and threats on the national security level, brand new business models and market environments, as well as the new 'culture' of online communities demanded the United States to adapt and change. Given their shortsighted nature, the old patchwork of legislation during the previous era could not guide the U.S. through such transformation. Therefore, it was rather unfortunate that the U.S. had to start over again to redefine terms, work with new players and reestablish a new system from ground zero.

On the national security level, the U.S. shifted away from traditional security thinking and for the first time, under the Obama administration, highlighted cybersecurity as one of the primary national security priorities to the U.S. This refreshed and expanded definition of national security paved the way for various transformations of U.S. military structure, combat theories and resource distribution. That said, the efforts to shift the focus from traditional security threat to new security threat in the short-time period inevitably failed to maintain the balance between short-term and long-term objectives which made it very difficult to maintain consistent long-term planning when new concerns emerge a decade later in the 2020s.

Under the Obama administration, the U.S. reorganized its cyber forces and created the United States Cyber Command on May 21, 2010.[10] This new military command was established during a period when military operation in cyber space became an innovative way of warfighting around the first decade of the 21st century. While Russia, and occasionally China, still emerge in official U.S. documents as major challengers or security threats during the early 2010s, Washington's top security concerns remain to be non-state actors or state actors adopting asymmetric warfare tactics that could level U.S. military superiority. In fact, in its 2015 National Security Strategy, the Obama administration put cybersecurity ahead of the aggression by Russia and climate change as it laid out America's top security priorities.[11]

In addition, cyber warfare also proved to be a useful means to counter challengers without putting boots on the ground or calling in inaccurate drone strikes. The Obama administration launched the world's first publicly known cyber attack on Iran's nuclear program in 2012,[12] in an attempt to slow down Tehran's development of nuclear weapons at the time. Cyber warfare showed its potential and value during a period when the U.S. was dealing with nontraditional, asymmetric, and peacetime security challenges. However, as time changes and the concept of national security swings back to great power competition, the nature of national cybersecurity defense and, subsequently, competitors have gradually changed.

Russia is a traditional cybersecurity threat to the United States. Washington accuses Moscow of engaging in "malicious cyber activities to enable broad-scope cyber espionage" and suggests that the Kremlin is sponsoring various threat actors that target military, economic, energy, and entertainment industries, infrastructures, and organizations in the U.S.[13] However, the concern of Russian hacking and cyber attack reached a new level when 12 Russian military intelligence officers were charged with their "alleged roles in interfering with the 2016 United States elections"[14] through hacking and gaining unauthorized access into the computers of U.S. persons and entities involved in the 2016 election. The possibility that a hostile power could interfere with America's very fundamental democratic institutions raised the concern over cybersecurity to a new level. Cybersecurity, since the latter half of the 2010s, became not only a valuable military add-on, but also a necessary security imperative.

The need to strengthen and potentially reform U.S. cybersecurity capabilities also become imminent as Washington increasingly sees China as a "pacing challenger."[15] Washington identifies China as "the broadest, most active, and persistent cyber espionage threat to U.S. government and private-sector networks,"[16] which has the capability of launching cyber attacks that puts critical infrastructure in danger. The Trump administration, in 2018, launched the U.S.'s first cyber strategy since 2003. In this latest cyber strategy, it champions the defense of homeland networks, systems, functions, and data as top cybersecurity priority. The 2018 strategy also name dropped China for engaging "cyber-enabled economic espionage and trillions of dollars of intellectual property theft."[17] Given Washington's longtime grievances towards China's alleged economic espionage and intellectual property (IP) theft, the efforts to cope with China in the cyber realm will only intensify, especially as the modern warfighting concept becomes increasingly reliant on joint operations in the cyber domain. However, that also means that the traditional cybersecurity priorities, particularly those concerning non-critical economic activities such as digital trade, will fall out of the scope of national cybersecurity.

Google CEO Sundar Pichai testifies during a House Judiciary Committee hearing on Capitol Hill in Washington, DC, December 11, 2018. - Google chief executive Sundar Pichai was grilled by US lawmakers over allegations of "political bias" by the internet giant, concerns over data security and its domination of internet search.
(Source: SAUL LOEB/AFP via Getty Images)

In their 2023 National Cybersecurity Strategy, the Biden-Harris administration has revised the approach under the Obama and Trump administration and suggested that they will "rebalance the responsibility to defend cyberspace" and "shape market forces to drive security and resilience" at the same time.[18] While defending America's critical economic and cyber infrastructure remains at the core of U.S. national cybersecurity, the Biden-Harris administration specifically pointed at the big companies, "those within our digital ecosystem", to promote non-critical cybersecurity areas such as privacy and personal data protection. This puts a big question mark on whether the U.S. businesses, especially the Big Tech companies could properly coordinate with the government to manage cybersecurity accordingly.

On business practices, the nature of laissez-faire governance in the United States, coupled with the rapid expansion of Big Tech companies in terms of business practices, size and influences, made it impossible for the U.S. to develop any kind of framework that can timely address concerns and problems that emerged during this period. In direct contrast to the drastic amount

of new problems and concerns, the United States became increasingly unable to develop new 'patches,' let alone in time.

Internationally, the U.S. business approach that was developed in the U.S. laissez-faire governance culture encountered problems since the late 2000s, as they attempted to enter markets that had more systematic regulations or stronger government oversight. In the end, U.S. companies were faced with two options: adapting to these new types of markets, or exiting despite business potentials.[19] As the former meant costly business model transition and the latter meant lost growth opportunities, both represented difficult business choices. As economic development triumphs at the time, the U.S. chose to support the expansion of American businesses into new markets through repeatedly calling for openness, transparency, and integration, thus sweeping under the rug the concerns for data governance coordination among allies and trading partners. In 2008, the United States led the efforts towards the Seoul Declaration, in which more than 30 countries committed to support "the free flow of information" and uphold the "open, decentralized and dynamic nature of the Internet."[20] In 2011, one year after Google failed to reach an agreement with Beijing to coordinate its data practices and legal compliance in China, the United States demanded information from China's "Internet restrictions," arguing that they created "commercial barriers" that hurt American businesses.[21] In 2013, U.S. policymakers reportedly launched "an unprecedented lobbying campaign" against the European Union's plan to enact an EU Data Protection Regulation.[22]

However, the decision to prioritize American businesses' overseas expansion came with a regulatory consequence at home. Given the laissez-faire tradition and the bottom-up approach, the need to lay down the data governance foundation and prepare for future data challenges had to be either delayed or to make way for more pressing policy objectives. That said, the positive notion during this period is that both the government, Congress and the businesses had begun extensive, active, albeit less constructive discussions over a wide range of questions and concerns, some of which have become key issues at present. In 2012, the Federal Trade Commission (FTC) called on companies to adopt better data privacy and protection practices.[23] In 2014, FTC recommended that Congress enact legislation to tighten governance over "data brokers" and protect consumer rights.[24] However, despite the call from FTC to both the industry and Congress, data privacy and protection on the federal level have remained 'discussions' until May, 2023. On the other hand, concerns for the growing power of the big tech platforms and relevant antitrust actions emerged as early as the 2000s.[25] However, despite individual cases and actions on Microsoft, Google and Facebook (now Meta),[26] a systematic policy shift, whether through judicial, legislative, executive or private industrial practices, remained an open debate and an objective yet to be achieved by U.S. data governance.[27] As U.S. policymakers support American businesses overseas, regulators have demanded businesses to cooperate domestically in exchange. In this vein, there were constant

negotiations and exchanges between Big Tech and policymakers. At the same time, given the rapid business expansion and technological developments of the Big Tech companies, the industry was and continues to be constantly evolving, creating new concerns, new demands and new issues to bargain for. By mid- to late- 2010s, the United States has had limited to none new data governance measures despite the heated, consistent public, stakeholder and international discussions on various concerns and problems.

President of the European Parliament Antonio Tajani met Facebook CEO Mark Zuckerberg to discuss data privacy on May 22, 2018.
(Source: European Parliament; CC BY-NC-ND 2.0)

The consequences of delaying or overlooking data governance developments became most notable in the transatlantic mechanism to facilitate data flows. Since 2000, the U.S. and EU established the Safe Harbour Framework to facilitate data flows across the Atlantic by ensuring that companies on both sides adhere to the same standards of data protection. In October, 2015, the European Court of Justice invalidated the Framework, holding that U.S. protection of data was inadequate. In response, a new framework, the EU-U.S. Privacy Shield Framework was established.[28] Nevertheless, in July, 2020, the Court of Justice of the European Union again ruled that the U.S. data protection laws were not adequate enough to ensure that companies in the U.S. are bound to offer personal data protection equivalent to those in Europe.[29] As the United States lacks an adequate data privacy and protection regime in the eyes of the European Court of Justice, American businesses have faced waves of uncertainties and higher compliance burden if they hope to transfer data to and from the European Union.

Notably, data hack protection was one of the very few areas where the United States made tremendous progress in the first two decades of the 21st century. The concerns over data protection were shared across different levels of decision-making and among stakeholders. Early cases of data breaches and leaks ran alarms across U.S. businesses. In 2005 and 2006, Wal-Mart encountered two data breaches in which sensitive sales data and internal codes were found to be breached and leaked to a computer in Eastern Europe.[30] In 2014, JP Morgan Chase said that the bank experienced a data breach that affected the accounts of more than 76 million American households.[31] Business espionage and state-backed hacking pressured the U.S. government to join hands with businesses to develop proper data protection mechanisms and rules, starting with raising awareness of the danger of data threat. The U.S. market is thus well-educated about the importance of data protection and subsequently, the importance of privacy protection. That said, due to the lack of interest in international coordination, the U.S. standard is narrowly focused on domestic issues, which has led to more controversies about cross-border data protection as digitalization further globalizes. The rise of cloud computing in the early 2010s, for example, has raised concerns among U.S. policymakers on international data policy as well as the domestic regulatory frameworks in countries such as China and India.[32]

On personal rights and data privacy, the call towards a baseline federal data privacy regime has lasted for at least 20 years, supported by the Federal Trade Commission, the primary enforcer of the 'patchwork' of U.S. data laws as well as leading data privacy and civil rights advocates.[33] However, despite multiple hearings spanning across the last two decades,[34] progress beyond debates and discussions was limited. As is detailed in 2021 by Jessica Rich, a longtime FTC official and privacy law advocate, very few American Big Tech disclosed their data collection and usage practices although they clearly collect massive amounts of sensitive and personally identifiable data on a daily basis.[35] Given the sheer black box, it is even more difficult to ensure that consumers have the right over how their data are collected, used and profited from. Despite the severity and scope of the issue, federal lawmakers and policymakers have not taken any concrete steps since the 2000s.

Despite the fact that data-based businesses have pioneered the development of U.S. economy during the first decade of the 21st century, the approach to data governance and regulations has not changed much compared to 1970. The same patchwork mentality, together with the laissez-faire approach inspired by promising and rapid business growth, made any forward-thinking system-building efforts costly compared to short-term patchworks or the choice to kick the can down the road. While some may argue that this is a period of missed opportunity for a U.S. data governance framework, it is not necessarily the case. The American laissez-faire approach, together with its bottom-up framework, ensured that the business could grow without restrictions and therefore maximized the efficiency of business development. Efforts

to promote the growth of Big Tech firms is not wrong by nature. What is unfortunate is that the other competitors—China and EU—also managed to catch up to U.S. Big Tech development and became pacing challenges to the U.S. leadership in the digital economy and technology development. Data governance, protection and its associated standard making were not a necessity should the U.S. sustain its prestigious position in the international system. However, it became an absolute top priority due to two pacing challenges that are well-equipped with forward-thinking, comprehensive systems guided by top-down policy guidance. When the clock turns to the third decade of the 21st century, data governance and protection became more than a subject matter of regulating business and reprimanding ill practices—it is also a matter of international leadership based on rule- and standard-making.

PART 3

TikTok and China: When the American Catch-up Turned Hysterical

On March 23, 2023, the U.S. House of Representatives brought before its Energy and Commerce Committee TikTok CEO Shou Zi Chew to testify on the social media platform's data security practices.[36] With extensive media coverage surrounding the hearing,[37] the Committee aimed to scrutinize the company's ties to the Chinese government as well as to understand how "Big eTech companies, like TikTok" utilize "harmful" "aggressive" algorithms that disregard user safety and exploit users for profit.[38] In the end, the hearing presented a mix of two concerns. On the one hand, Chew was repeatedly questioned over TikTok's connections with the Chinese government and the extent to which TikTok would be obliged to transfer U.S. user data to Chinese authorities. On the other hand, lawmakers raised concerns about TikTok's data collection practices as well as the impact of the app's content moderation policy on users, especially children. Concerning the former, Chew repeatedly denied the company's ties to China but failed to convince the lawmakers. Concerning the latter, Chew argued that TikTok was no different than "many other companies in our industry."

Washington's concern for TikTok is nothing new. In August, 2020, then U.S. President Donald Trump issued an executive order to block the social media app TikTok and Chinese messaging app WeChat from the United States.[39] To the Trump administration, TikTok posed a national security threat because it could grant the Chinese government access to massive amounts of U.S. user data—unless TikTok's U.S. operation was sold to an American company, there could be no protection and no guarantee even if the user data were currently stored in U.S. servers. The Biden administration took a similar, but potentially more comprehensive approach. Although dropping the specific ban on TikTok, U.S. President Joe Biden ordered a national security review of social media apps connected to China.[40] In June 2021, the Biden administration announced that "connected software applications" that are "designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary [which include China]" are deemed to be a threat to "the national security, foreign policy, and economy of the United States" and issued a list of potential indicators of risk relating to connected software applications of foreign origin.

With the introduction of the RESTRICT Act in Congress, both the Biden administration and the current Congress showed the intent to eye an even more strict and comprehensive approach.[41]

When looking at the hearing issue by issue, many of the concerns referred to in the TikTok probe do not seem new. They are the same grievances and issues levied towards the U.S. Big Tech companies during the first two decades of the 21st century. However, it is the nature of TikTok—a Chinese-owned transnational technology company—that has complicated the entire situation. Managing the TikTok case not only created a precedent for new demands towards data governance in the new era, but also established a precedent of the U.S. executing its own authority to create a new 'rule of the game' amid strategic competition with China.. Nevertheless, the overall toxic environment caused by U.S.-China competition over-securitized the TikTok issue and distorted the policy reaction to other data governance matters that gained new significance in the new era but have a history of being overlooked or intentionally ignored in the previous decades.

TikTok CEO Shou Zi Chew prepared to testify before the House Energy and Commerce Committee hearing on March 23, 2023.
(Source: Tasos Katopodis/Getty Images)

Although concerns for Big Tech data practices and content moderation were most pronounced in the TikTok discussion, similar issues were already present through the individual practices of Big Tech companies and through efforts towards a comprehensive data privacy regime. In parallel to congressional concerns about TikTok's data practices, U.S. regulators, users and

advocacy groups have long voiced concerns about individual practices of Facebook (now Meta), among other Big Tech companies. Data privacy practices of Facebook first led to user backlash in late 2006, when Facebook decided, without notice and opt-out options, to curate each user's posts into a daily feed for their Facebook friends.[42] In 2011, the Federal Trade Commission (FTC) found that Facebook failed to follow through with its own privacy policy, including promises that users' private information will not be made public without notice, or that third-party apps would only access user data that are necessary to the apps' operations.[43] Although these individual cases were more or less addressed, including through Facebook's promise to go through a data privacy check with the FTC every two years, new concerns and new problems have left previous precedents inapplicable as the technology industry develops new features and new kinds of algorithms. In 2018, Facebook acknowledged that political consulting firm Cambridge Analytica had misused tens of millions of Facebook user data before and during the U.S. general election.[44] In 2021, former Facebook product manager Frances Haugen testified in front of the U.S. Senate Committee on Commerce, Science and Transportation, arguing that Facebook's algorithms and business practices deliberately prioritize profits over user safety or the prevention of extremism and online hate.[45]

Alarmed and inspired by the European Union's strict General Data Protection Regulation (GDPR), and witnessing the inaction of the federal government, the state government of California decided to pass the California Consumer Privacy Act of 2018 (CCPA), which offers GDPR-like data privacy protections to consumers in California.[46] Under CCPA, individuals are

Fortinet founder, Chairman and CEO Ken Xie, Profound Impact Corp. Founder and President Sherry Shannon-Vanstone, and IBM Cognitive Solutions Senior Vice President David Kenny discussed data stewardship for a digital age at Fortune Global Forum 2018.
(Source: FORTUNE Global Forum; CC BY-NC-ND 2.0)

granted the right to sue companies for data breaches, ensures an easy way to opt-out of all data collection, and creates a new state agency to enforce its measures. Although CCPA is hailed as an example of progressive data privacy legislation in the United States, the progress achieved by the act is limited by a multitude of factors. First, enacted by the state government of California, it only applies to one of the 50 states in the United States. (Admittedly, given the number of Big Tech companies that are based in California, CCPA standards likely apply to and impact many out-of-state consumers of Big Tech services.) Second, although some other state governments seemingly followed suit, many chose to follow the Virginia model, a law that was originally authored by Microsoft with input from Amazon. In contrast to CCPA, Virginia's law does not include a private right to sue, preserves a manual opt-out approach, and grants enforcement powers only to the state attorney general.[47] While industry stakeholders are not completely united around weaker legislation (with firms like DuckDuckGo, Yelp, and Spotify supporting California's bill), the biggest players' support for Virginia's law has carried a great deal of weight and most state-level data laws which are in the drafting process mirror Virginia's law rather than California's.[48] [See Appendix B for a detailed side-by-side comparison of the state laws.] Thirdly, the existence of CCPA could in turn block the passage of the much-needed federal data privacy regime. Following the introduction of the American Data Privacy and Protection Act, California Governor Gavin Newsom, joined by state Attorney General Rob Bonta, and the California Privacy Protection Agency, argued that the law seeks to "replace California's landmark law," i.e. CCPA, "with weaker protections."[49] In an earlier letter to congressional leaders, attorney generals of California, Connecticut, Illinois, Maine, Massachusetts, Nevada, New Jersey, New Mexico, New York and Washington state expressed similar concerns.[50] As state-level laws add another layer of complication to the spaghetti bowl or 'patchwork' of existing U.S. data governance, and hence regulatory costs and compliance burdens, state-level efforts reveal the dire need, rather than working as a part-time alleviation, for effective federal governance on both the regulation of Big Tech companies, and the sufficient protection of individual privacy rights.

The long-time lack of a consistent and effective data governance mechanism to chronic issues, together with the over-securitization and hysteria of the notion of U.S.-China competition, ultimately produced the Risk Information and Communications Technology (RESTRICT) Act, which has every single element that a forward-thinking, comprehensive and accurately targeted, capable legislation should avoid. Promoted as a "systematic framework for addressing technology-based threats to the security and safety of Americans,"[51] the RESTRICT Act proposes to grant the U.S. Department of Commerce expansive authority to investigate any technology- and "foreign adversary"-related business transactions with limited to none oversight. The Commerce Department is allowed to identify, investigate, prevent and mitigate any business transactions of products and services that primarily intended to process, store, communicate or display information—any social media, Internet and communications services

and products, among a wide range of other technology-based products and services—that are related to foreign adversaries, whether the nation, its companies or company subsidiaries. Noting traditional judicial deference to national security investigations, the RESTRICT Act explicitly exempted the Commerce Department from judicial review or record disclosure (i.e. Freedom of Information Act, or FOIA) obligations, whether or not confidential information is involved, with the exception of a narrow appeal process with a very high bar favoring the executive branch. Finally, the Commerce Department is authorized to require "complete information" related to its investigation, to mitigate national security risks through preventing and altering the transactions and is able to impose civil and criminal penalties for violating RESTRICT Act-related directions and orders. In short, the RESTRICT Act aims to grant the Commerce Department, the department that has traditionally been responsible for regulating such grave sanctions like the Entity List, unbridled power to investigate and regulate any tech-related business transactions that also relate to China.

What's lacking from such a "systematic framework to address discrete risks" (according to the White House National Security advisor Jake Sullivan) and a "comprehensive, risk-based approach that proactively tackles sources of potentially dangerous technology"[52] (according to the bill's congressional sponsors) was the identification of a specific and clearly defined group of challenges, to be coupled with systematic, consistent and forward-thinking policy solutions that can ideally evolve and adapt to foreseeable challenges of the future. Admittedly, the act identified several areas that the Commerce Department should focus on and among them are digital products that involve the data of more than 1 million users, e-commerce, surveillance, critical infrastructure and telecommunication. However, although the RESTRICT Act was incentivized by "China threats" such as TikTok, it is unclear which practices about TikTok the bill aims to address. As such, it would be even more unclear whether and how other Chinese companies should be regulated by the Commerce Department, let alone the business partners of these Chinese companies. With exceedingly expansive coverage of all data-related products and services, it certainly seems that the lawmakers are fearing the unknown of TikTok and the like, instead of having a clear plan to address known threats to the United States.

As the act aims to address "technology-based threats" from abroad, it naturally left the 'finer details' to the hands of the Commerce Department. These include the method to identify data-related challenges, the standards against which data practices should be regulated and the principles behind the regulation of (foreign) Big Tech industry. As regulatory rulings and practices can be easily changed under different department heads and administrations, especially when limited public or judicial oversight is granted, this meant that the RESTRICT Act framework would only produce rulings that lack consistency, predictability or accountability. As the Commerce Department is not required to disclose most of its administrative records and hence the basis of its regulations, it will also be extremely difficult for the United States to apply any RESTRICT Act practices and experiences beyond the technological competition

with China. As such, similar data concerns that were exposed through the Facebook incidents or through the introduction of state-level privacy acts would remain unresolved. Much like the late 2000s and 2010s practices to kick the can down the road, the groundbreaking RESTRICT Act merely kicked part of the can from Congress to enforcement officials and their inconsistent, case-by-case approach. Given the lack of any progress in improving U.S. data governance, it is thus unclear how the RESTRICT Act can promote American leadership in data and data standards.

Left: Sen. Mark Warner (D-Virginia), sponsor of the RESTRICT Act. (Source: U.S. Senator Mark Warner; U.S. government work/public domain) Right: Jake Sullivan, White House National Security Advisor under President Biden. (Source: Executive Office of the President of the United States; U.S. government work/public domain)

Although the RESTRICT Act was hailed as another manifestation of bipartisan efforts to jointly address U.S. strategic competition with China,[53] it can also be understood to reveal the sad reality that the highly divided U.S. political establishment could only be united against an overexaggerated foreign threat. In contrast to Washington's claim that there are technology-based risks to U.S. national security that require solutions such as the RESTRICT Act, there are already multiple and overlapping authorities aimed at preventing technology-related risks from China and other foreign adversaries. In May 2019, the Trump administration issued a wide-ranging Executive Order to "secure the information and communications technology and services supply chain," which granted the administration, as well as the follow-up Biden administration, extensive power to address the risks of new or prevailing "untrusted" information and communications products and services in the United States.[54] Throughout the Trump and the Biden administrations, the Committee on Foreign Investment in the United States (CFIUS) has appeared to work closely with TikTok and other entities to work on data-related risks, and

CFIUS specifically underlined sensitive personal data as a focal point for its review starting February 2020.[55] It is thus confusing, to say the least, when TikTok and technology-based threats were again singled out as a loophole that must be closed.

In contrast, the long-lasting loopholes that should have been closed long ago, e.g., a federal data privacy framework, have remained open despite consensus across the aisle. On July 20, 2022, the House Energy & Commerce Committee advanced the American Data Privacy and Protection Act (ADPPA), a comprehensive data protection and privacy act that gained overwhelming support from bipartisan lawmakers and was hailed as "a major step forward by Congress in its two-decade effort to develop a national data security and digital privacy framework."[56] The bill proposes to grant consumer rights such as the right to access, to correct and delete their data, to opt out of targeted advertising and to object before their data is transferred to the third party and to impose duties on data controllers such as the duty to disclose their data practices, to only collect data proportionate to the service requested by the consumer and to adopt reasonable data security practices. Although ADPPA fell short of passing either congressional chamber before the end of the 117th U.S. Congress, the bipartisan and bicameral momentum in support of a federal data privacy law continued in the beginning of 2023.[57] In an op-ed published on January 11, 2023, U.S. President Joe Biden called for "serious federal protections for Americans' privacy" by limiting ways to collect, use and share "highly personal data."[58] Several weeks later, a bipartisan group of lawmakers—including House Energy and Commerce Committee Chair Cathy McMorris Rodgers, Ranking Member Frank Pallone, Innovation, Data, and Commerce Subcommittee Chair Gus Bilirakis, and Subcommittee Ranking Member Jan Schakowsky—all expressed support for establishing a national data privacy standard through a federal legislation in the likes of the ADPPA.[59] Despite the high-level, bipartisan support, momentum for the legislation slowed down when TikTok became the policy focal point instead. On March 1, 2023, roughly three weeks before the TikTok hearing, the Innovation, Data, and Commerce Subcommittee of the House Committee on Energy and Commerce held a hearing on ADPPA.[60] Since then, the bill has remained under consideration by the House Committee on Energy and Commerce for three months—even as the committee had passed another version of ADPPA nearly unanimously in the 117th Congress.[61]

With delays in even widely supported bills such as ADPPA, it is no surprise that urgently needed yet controversial reforms received even less progress, namely, the ongoing efforts within Congress to push Big Tech companies to take greater responsibility for the content they spread and the algorithms they use by reforming Section 230 of the Communications Decency Act of 1996. Enacted as part of the Communications Decency Act of 1996, Section 230 offers significant immunity to online platforms and website hosts in their moderation of contents published by third-party. Under Section 230(c)(1) and relevant judicial interpretations, online platforms are not (civilly) liable for exercising their "editorial functions," including "deciding whether to publish, withdraw, postpone or alter content."[62] Furthermore, under 230(c)(2),

U.S. President Joe Biden delivered his State of the Union address on February 7, 2023. The speech covered the need to pose stricter limits on Big Tech's data collection practices. (Source: The White House; U.S. government work/public domain)

good faith actions to restrict access to "lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" materials also do not generate civil liability. Thus, with limited statutory exceptions, Internet companies are provided with wide discretion to moderate third-party contents posted on their platform—free from the risks and impacts of civil actions initiated by their users, impacted individuals as well as federal and state agencies.[21]

Although proponents of Section 230 have argued that the law established a right balance between free speech and content moderation online,[63] Section 230 has turned from a protector of Internet innovation to an overly expansive shield protecting the already powerful Big Tech companies. Section 230 provided Big Tech platforms, such as Facebook (now Meta) and Google, a license and cover for their unclear and inconsistent moderation practices. It also allowed platforms to take the proliferation of illicit and harmful contents online less seriously and oftentimes leaves victims without much or any civil remedies. As U.S. President Joe Biden himself identified in his January 11, 2023 op-ed, Big Tech companies nowadays are responsible for creating "toxic echo chambers" of "extreme and polarizing content" and for allowing "abusive and even criminal conduct, like cyberstalking, child sexual exploitation, nonconsensual pornography, and sales of dangerous drugs."[64] Accordingly, Biden called on "Democrats and Republicans" to reform Section 230 and make Big Tech companies "take responsibility for the content they spread and the algorithms they use." In Congress, legislative proposals to reform Section 230 have come from both sides of the aisle and both chambers. [65]Nevertheless, these reform proposals provide a wide range of differing solutions to the Section 230 problem and reaching a point of consensus on these reforms has been hard to come by though on Capitol Hill. Not surprisingly, the issue was again kicked down the road after some talks and no movement.

2 Section 230's immunity does not apply when federal criminal statutes or intellectual property laws are concerned, or when states "enforce any state law that is consistent with [Section 230]." Since 2018, Section 230 no longer applies to federal civil actions and state criminal prosecutions related to certain sex trafficking laws. Allow States and Victims to Fight Online Sex Trafficking Act of 2017, U.S. Public Law 115-164, April 11, 2018.

Faced with the rapid changing of data practices across all sectors and fields, the United States faces a multitude of data governance challenges in the third decade of the 21st century. On the national security level, economic security during an era sans major power competition surpassed territorial and geopolitical security issues and became the U.S. government's top priority in security policy making. On the business level, as the protection of critical business secrets amid threats from state-backed and non-state-backed business espionage and unfair practices has become a top priority for transnational corporations, Washington has the responsibility to answer the calls from industry and protect American competitiveness. On the individual level, the increasing amount of Internet devices and the spread of smartphones have changed the way of life of ordinary individuals. Meanwhile, the long unresolved data governance issues, coupled with emerging concerns, calls for a sophisticated, systematic and comprehensive data protection and privacy regime amidst mass data collection and Big Tech malpractices.

However, while the different levels of concerns and issues should be addressed separately, equally and with care, recent cases suggest that the United States tends to choose to prioritize the more ideological and geopolitically-based China rhetoric when its domestic data governance concerns collide with international affairs of security and U.S.-China competition. As the TikTok hearing has shown, lawmakers have tended to often emphasize the app's "unique algorithmic design," hoping to single out the Chinese-owned TikTok from other Big Tech companies and address this one single "foreign adversary threat."[66] However, such efforts tend to translate into crude and redundant responses such as the RESTRICT Act, and incentivize political gestures over policy solutions. The latter would be exemplified by Montana's recent decision to ban TikTok from the state, a move that does not address root cause and systematic data problems, rattles businesses and communities and raises concerns among sound practitioners and experts.[67] As such, actions to address genuine concerns about American Big Tech are delayed, overlooked or intentionally kicked down the road.

Conclusion

As the United States moves into the third decade of the 21st Century, policymakers and lawmakers have come to realize the imminent need to reform the existing 'patchwork' approach to data governance in the United States in favor of a more systematic framework.[68] However, efforts to reform the domestic data governance system are complicated by national security concerns and the strategic imperative to outcompete China, especially as the United States feels the pressure to catch up to China and Europe on data governance and corresponding global rulemaking. As is evident from the stalled legislative process of the American Data Privacy and Protection Act (ADPPA), the United States' halfway efforts and incomplete plan towards an effective data governance system are no longer the result of the lack of policy consensus or political will. Instead, it is the internal friction that has stalled concrete progress with Washington torn between two priorities: the desire to address short-term China threats and the need to enact long-term, systemic data governance structures. As recent years have shown, the former often distracted and misled considerable momentum in the latter.

To unravel itself from the current dilemma, Washington should first cool down the overall political atmosphere and draw a clear distinction between genuine concerns about China and hysterical "Sinophobia." When genuine, long-term and strategic policy concerns are involved, the United States should establish a candid and constructive internal discussion among policymakers; business and industrial stakeholders as well as civil rights advocates and individual users. With all of the voices and concerns heard and addressed, a proper domestic consensus should be formed to address genuinely shared concerns, which will in turn serve as a solid foundation for a more responsible and well-managed strategy in U.S. data governance. With a shared goal towards American competitiveness and leadership, voices and interests should be united towards the long-time prosperity of U.S. data and technology industry, and effective data governance is a necessary element.

Additionally, Washington should understand and internalize the fact that not every data policy concern is about China. Although it is a valid political technique to use China to rally political support, such an approach is short-term, short-sighted and comes with a price. Without proper engagement and communication and, to some extent, coordination with China on data governance, the United States will be left with a unilateral data governance approach that has a single, limited scope and objective of targeting Chinese businesses. This approach

does no good to either the United States or China, and it risks impacting other global markets and standard-setting efforts such as those in the European Union and those under the Digital Economy Partnership Agreement (DEPA).

Meanwhile, businesses were the driving force for changes and reform in U.S. history, and they should continue to serve as a driving force for U.S. data governance system reform. As regulatory efforts ultimately aim to ensure the healthy growth and security of the data and technology industry, stakeholder engagement and coordination are essential elements of any policy actions and rulemaking process. As the 2023 National Cybersecurity Strategy indicated, the best actors to contribute to the work of closing loopholes are those who are within the U.S. digital ecosystem. At this moment, it is even more important to work with the businesses and ensure they become the driving force to inspire changes, rather than attempting to 'discipline' them and limit industrial support. Big Tech companies should be seen as potential partners rather than enemies or trespassers, even if candid and difficult conversations must be had to ensure the right balance between government regulation and industrial growth.

Moreover, China is not a viable excuse to cover up the shortcomings of U.S. data governance, whether on cybersecurity, business or privacy. While China does present a cybersecurity threat to the U.S., this was due to the fact that modern warfare has become heavily reliant on operations in the cyber domain, not because China's development in the cyber and digital realm serves as an act of aggression against the U.S. Washington should learn to walk a fine line between strengthening its own cybersecurity capabilities and allowing regular digital business to operate between China and the U.S. Both countries are the biggest drivers for the global digital economy, and the U.S. should not cut off one of its helping hands when it needs both China and the EU to help coordinate and transform the U.S. economy.

In order to promote and properly guide the development of data-related businesses, U.S. policymakers will need to pick between two choices. Option one, they can give a thorough, rational thought on establishing a self-evolving framework prepared for long-term concerns, foreseeable issues and future growth, one similar to the Chinese and the European model. With such a framework established and running, the policy discussion over data governance can afford to shift attention to national security concerns and laser-focus on pacing challenges such as China. Option two, to learn from history and avoid engaging in partisan politics or a patchwork mentality, U.S. policymakers can seek to provide a more business-friendly environment to ensure that the benefit of data-associated businesses surpass the costs and risks they generate to the general public and society. As such, the issue of data governance can afford to be swept again under the rug, and Congress and the White House can resume their routine business to deal with China. But either way, the building of domestic consensus will be a must and singling out Big Tech businesses as the enemy is not the right solution—whether they are American giants such as Facebook/Meta, or rising Chinese businesses such as TikTok.

Appendices

Appendix A: Notable Data Privacy Laws in the U.S., 1970s to 2000s

Year	Legislation	Applies to...	Summary of Relevant Provisions
1970	Fair Credit Reporting Act	Consumer credit reports and consumer reporting agencies	Consumer reporting agencies have the duty to investigate information disputed by the consumer, the duty to notify the consumer when an adverse action is taken on the basis of credit reports and the duty to only disclose information in the credit report for purposes specified in the Act.
1974	The Family Educational Rights and Privacy Act	Educational institutions that receive federal funding	Parents have the right to inspect, review, challenge and limit disclosure of their children's educational records.
1974	The Privacy Act	U.S. government	The Act establishes requirements and guidelines for government agencies in their collection, maintenance, use and dissemination of personally identifiable data of individuals.
1978	Right to Financial Privacy Act	U.S. government	The Act limits the ability of the U.S. government to obtain an individual's financial information, and requires legal notice or the individual's written consent except in law enforcement investigations and other limited exceptions.
1984	The Cable Communications Policy Act	The cable television industry	Section 631 of the "miscellaneous provisions" stipulates that: ▪ A cable operator should only collect personally identifiable information from consumers when such collection is necessary for providing the cable service. ▪ A cable operator must also provide a written statement to the consumer on how such information is collected and used.
1994	Driver Privacy Protection Act	Public driving license databases	The Act prohibits the disclosure of personal information in the public driving license databases without the express consent of the individual

Year	Legislation	Applies to...	Summary of Relevant Provisions
1996	Health Information Portability and Accountability Act	Patient health information	The US Department of Health and Human Services is authorized to establish national standards to protect sensitive patient health information and to develop privacy and security rules for such purposes.
1998	Children's Online Privacy Protection Act	Collection of children's data online	The Federal Trade Commission is instructed to develop regulations and guidelines for commercial websites and online services regarding the collection, use and disclosure of children's personal information.
1999	The Gramm-Leach-Bliley Act	Financial institutions	The bill requires relevant financial institutions to disclose their information-collection and sharing policies to their customers and to develop proper procedures to safeguard their customers' sensitive information.
2002	The E-Government Act	U.S. government	The bill responds to technological advances in computer, digitalization and the Internet service and creates additional government duty in the protection of personal information contained in government records and systems.
2002	The Federal Information Security Management Act	U.S. government	The bill establishes data security guidelines and standards through which the U.S. government and agencies are to protect government information and operations.
2009	Health Information Technology for Economic and Clinical Health Act	Patient health information	The bill incentivizes the usage of electronic health record systems and widens the scope of the 1996 Health Information Portability and Accountability Act with regard to electronic health record systems.

Appendix B: Summary of State-level Data Privacy Laws (California, Virginia, Colorado, Utah and Connecticut)

State	California	Virginia	Colorado
Data Privacy Law (in order of enactment)	CCPA (as amended by CPRA)	VCDPA	CPA
Effective Date	January 1, 2023 (original statue effective January 1, 2020)	January 1, 2023	January 1, 2023
Applicability	"Businesses" in California meeting one of three thresholds: 1. Annual revenues over $25,000,000 2. Collect personal information of over 100,000 consumers or households 3. Generate at least half of revenues from sales of personal information	"Controllers," persons that conduct business, that produce products or services directed towards state residents and: 1. Control or process personal data of more than 100,000 resident's data per year 2. Derive more than half of revenues from the sale of personal data of at least 25,000 residents	"Controllers," persons that conduct business, that produce products or services directed towards state residents and: 1. Control or process personal data of more than 100,000 resident's data per year 2. Derive revenue from the sale of personal data of at least 25,000 residents
Exemptions	1. Information (not institutions) subject to GLBA or California financial privacy laws 2. Institutions/ information subject to federal regulations (ie. HIPAA) 3. Non-profit organizations	1. Personnel data 2. Business-to-Business information 3. Institutions/ information subject to federal regulations (ie. HIPAA) 4. Financial institutions subject to the GLBA 5. Non-profit organizations	1. Personnel data 2. Business-to-Business information 3. Institutions/ information subject to federal regulations (ie. HIPAA) 4. Financial institutions subject to the GLBA 5. Data maintained by state universities
Consumers' Rights of Access, Correction, Portability, Deletion, and Opting Out of Ads/Sales	Yes	Yes	Yes
Opt-in or Opt-out of Processing Sensitive Data	Opt-out	Opt-in	Opt-in
Controller Requirement to Carry Out Data Protection Impact Assessments	Yes	Yes	Yes
Right of Private Individuals to Sue Data Controllers	Yes	No	No
Enforcement	California Privacy Protection Agency (independent), Attorney General	Attorney General	Attorney General and District Attorneys

Appendix B: Summary of State-level Data Privacy Laws (California, Virginia, Colorado, Utah and Connecticut)

Utah	Connecticut	State
UCPA	CTDPA	**Data Privacy Law (in order of enactment)**
December 31, 2023	July 1, 2023	**Effective Date**
"Controllers," persons that conduct business, that produce products or services directed towards state residents and: 1. Have an annual revenue of over $25,000,000 2. Control or process personal data of more than 100,000 resident's data per year 3. Derive more than half of revenues from the sale of personal data of at least 25,000 residents	"Controllers," persons that conduct business, that produce products or services directed towards state residents and: 1. Control or process personal data of more than 100,000 resident's data per year 2. Derive more than a quarter of revenues revenue from the sale of personal data of at least 25,000 residents	**Applicability**
1. Personnel data 2. Business-to-Business information 3. Institutions/ information subject to federal regulations (ie. HIPAA) 4. Financial institutions subject to the GLBA 5. Non-profit organizations	1. Personnel data 2. Business-to-Business information 3. Institutions/ information subject to federal regulations (ie. HIPAA) 4. Financial institutions subject to the GLBA 5. Non-profit organizations	**Exemptions**
Yes	Yes	**Consumers' Rights of Access, Correction, Portability, Deletion, and Opting Out of Ads/Sales**
Opt-out	Opt-in	**Opt-in or Opt-out of Processing Sensitive Data**
No	Yes	**Controller Requirement to Carry Out Data Protection Impact Assessments**
No	No	**Right of Private Individuals to Sue Data Controllers**
Attorney General	Attorney General	**Enforcement**

Endnotes

1 U.S. Library of Congress, Congressional Research Service, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh, R45631 (2019); "State Leadership on Data Privacy Creating Regulatory Patchwork," *Lexis Nexis*, March 16, 2023, https://www.lexisnexis.com/community/insights/legal/capitol-journal/b/state-net/posts/thought-leadership-creating-regulatory-patchwork; "Understanding the patchwork of US data privacy laws," *Security*, June 15, 2022, https://www.securitymagazine.com/articles/97810-understanding-the-patchwork-of-us-data-privacy-laws.

2 See, e.g. Whalen v. Roe, 429 U.S. 589, (1977), Griswold v. Connecticut, 381 U.S. 479, 485 (1965), NASA v. Nelson, 562 U.S. 134, 159 (2011).

3 "The Privacy Act of 1974," U.S. Office of Special Council, accessed May 30, 2023, https://osc.gov/Pages/Privacy-Act.aspx.

4 "Privacy Act of 1974," Office of Privacy and Civil Liberties, U.S. Department of Justice, updated October 4, 2022, https://www.justice.gov/opcl/privacy-act-1974; "The Privacy Act of 1974," U.S. Office of Special Council.

5 See, e.g., the categorization of the Privacy Act of 1974 by the U.S. Office of Special Counsel, the U.S. Department of Justice, or the U.S. Department of Treasury. "The Privacy Act of 1974," U.S. Office of Special Council; "Privacy Act of 1974," U.S. Department of Justice; "Privacy Act," U.S. Department of the Treasury, accessed May 30, 2023, https://home.treasury.gov/footer/freedom-of-information-act.

6 "Health Insurance Portability and Accountability Act of 1996 (HIPAA)," Centers for Disease Control and Prevention, last reviewed June 27, 2022, https://epic.org/dppa/; "The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record," Electronic Privacy Information Center, accessed May 30, 2023, https://www.cdc.gov/phlp/publications/topic/hipaa.html.

7 "How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act," Federal Trade Commission, July 2002, https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.

8 See guidelines available at "Privacy and Security," Federal Trade Commission, accessed May 30, 2023, https://www.ftc.gov/business-guidance/privacy-security.

9 Daniel J. Solove and Woodrow Hartzog, *Breached!: Why Data Security Law Fails and How to Improve It* (Oxford: Oxford University Press, 2022); "Facebook, Inc., In the Matter of," FTC File Number 092 3184, Federal Trade Commission, April 28, 2020, https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter.

10 "Our History," U.S. Cyber Command, accessed May 30, 2023, https://www.cybercom.mil/About/History/.

11 Barack Obama, *National Security Strategy* (Washington D.C.: The White House, 2015), February, https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf.

12 Ellen Nakashima and Joby Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say," *The Washington Post*, June 2, 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

13 "Russia Cyber Threat Overview and Advisories," Cybersecurity & Infrastructure Security Agency, accessed May 30, 2023, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia.

14 "Russian Interference in 2016 U.S. Elections," Federal Bureau of Investigation, poster, accessed May 30, 2023, https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections.

15 David Vergun, "China Remains 'Pacing Challenge' for U.S., Pentagon Press Secretary Says," U.S. Department of Defense News, November 16, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2845661/china-remains-pacing-challenge-for-us-pentagon-press-secretary-says/.

16 "China Cyber Threat Overview and Advisories," Cybersecurity & Infrastructure Security Agency, accessed May 30, 2023, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china.

17 Donald J. Trump, *National Cyber Strategy of the United States of America* (Washington D.C.: The White House, 2018), September, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

18 "FACT SHEET: Biden-_Harris Administration Announces National Cybersecurity Strategy," The White House, March 2, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

19 Sissi Gao, "Google Shuts Down One of Its Last Remaining Services in China as Big Tech Exits the Country," *Observer*, October 3, 2022, https://observer.com/2022/10/alphabet-shut-google-translate-china-big-tech/.

20 *The Seoul Declaration for the Future of the Internet Economy*, declared at the OECD Ministerial Meeting on the Future of the Internet Economy, at Seoul, Korea, June 17-18, 2008, https://www.oecd.org/digital/consumer/40839436.pdf.

21 "United States Seeks Detailed Information on China's Internet Restrictions," Office of the United States Trade Representative, October 19, 2021, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2011/october/united-states-seeks-detailed-information-china%E2%80%99s-i.

22 Zack Whittaker, "Privacy groups call on US government to stop lobbying against EU data law changes," ZDNet, February 3, 2013, https://www.zdnet.com/article/privacy-groups-call-on-us-government-to-stop-lobbying-against-eu-data-law-changes/.

23 "FTC Issues Final Commission Report on Protecting Consumer Privacy," Federal Trade Commission, March 26, 2012, https://www.ftc.gov/news-events/news/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

24 "FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information," Federal Trade Commission, May 27, 2014, https://www.ftc.gov/news-events/news/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more-transparent-give-consumers-greater.

25 Peter Swire, "Protecting Consumers: Privacy Matters in Antitrust Analysis," Center for American Progress, October 19, 2007, https://www.americanprogress.org/article/protecting-consumers-privacy-matters-in-antitrust-analysis/.

26 Joel Brinkley, "U.S. vs. Microsoft: The Overview; U.S. Judge Says Microsoft Violated Antitrust Laws with Predatory Behavior," *The New York Times*, April 4, 2000, https://www.nytimes.com/2000/04/04/business/us-vs-microsoft-overview-us-judge-says-microsoft-violated-antitrust-laws-with.html; "Justice Department Requires Six High Tech Companies to Stop Entering into Anticompetitive Employee Solicitation Agreements," The United States Department of Justice, September 24, 2010, https://www.justice.gov/opa/pr/justice-department-requires-six-high-tech-companies-stop-entering-anticompetitive-employee; Mark Scott, "E.U. Fines Facebook $122 Million Over Disclosures in WhatsApp Deal," *The New York Times*, May 18, 2017, https://www.nytimes.com/2017/05/18/technology/facebook-european-union-fine-whatsapp.html.

27 Biden, "Republicans and Democrats, Unite Against Big Tech Abuses"; Samuel Miller, "If Google Is A 'Bad' Monopoly, What Should Be Done?," *FedArb.com*, January 1, 2013, https://www.fedarb.com/wp-content/uploads/2018/11/If-Google-Is-A-Bad-Monopoly-What-Should-Be-Done-Samuel-Miller-article.pdf.

28 "Privacy Shield Overview," Privacy Shield Framework, accessed May 30, 2023, https://www.privacyshield.gov/Program-Overview.

29 Frederick Saugman and Martin Braun, "European Court of Justice Rules US Privacy Shield Invalid," WilmerHale, August 11, 2020, https://www.wilmerhale.com/en/insights/blogs/wilmerhale-w-i-r-e-uk/20200811-european-court-of-justice-rules-us-privacy-shield-invalid.

30 Kim Zetter, "Big-Box Breach: The Inside Story of Wal-Mart's Hacker Attack," *WIRED*, October 13, 2009, https://www.wired.com/2009/10/walmart-hack/.

31 Dominic Rushe, "JP Morgan Chase reveals massive data breach affecting 76m households," *The Guardian*, October 3, 2014, https://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach.

32 Renee Berry and Matthew Resiman, "Policy Challenges of Cross-Border Cloud Computing," *United States International Trade Commission Journal of International Commerce and Economics* (May 2012), https://usitc.gov/journals/policy_challenges_of_cross-border_cloud_computing.pdf.

33 Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (Federal Trade Commission, 2000), May, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf; Jerry Berman, "Prepared Statement before the Senate Committee On Commerce, Science, And Transportation on the Federal Trade Commission's Report To Congress—'Privacy Online: Fair Information Practices In The Electronic Marketplace'," May 25, 2000, https://cdt.org/wp-content/uploads/testimony/000525berman.shtml.

34 Jessica Rich, "After 20 years of debate, it's time for Congress to finally pass a baseline privacy law," Brookings, January 14, 2021, https://www.brookings.edu/blog/techtank/2021/01/14/after-20-years-of-debate-its-time-for-congress-to-finally-pass-a-baseline-privacy-law/; Berman, "Prepared Statement"; Jesscia Rich, "Prepared Statement of the Federal Trade Commission on Discussion Draft of H.R.__, Data Security and Breach Notification Act Of 2015," Federal Trade Commission, March 18, 2015, https://www.ftc.gov/legal-library/browse/prepared-statement-federal-trade-commission-discussion-draft-hr__-data-security-breach-notification.

35 Rich, "After 20 years of debate."

36 "Full Committee Hearing: 'TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms'," hearing in front of the U.S. House Energy & Commerce Committee, March 23, 2023, https://energycommerce.house.gov/events/full-committee-hearing-tik-tok-how-congress-can-safeguard-american-data-privacy-and-protect-children-from-online-harms.

37 Catherine Thorbecke, "TikTok CEO in the hot seat: 5 takeaways from his first appearance before Congress," *CNN*, March 23, 2023, https://www.cnn.com/2023/03/23/tech/tiktok-ceo-hearing/index.html; David Shepardson and Rami Ayyub, "TikTok congressional hearing: CEO Shou Zi Chew grilled by US lawmakers," *Reuters*, March 24, 2023, https://www.reuters.com/technology/tiktok-ceo-face-tough-questions-support-us-ban-grows-2023-03-23/; Dell Cameron, "The TikTok Hearing Revealed That Congress Is the Problem," *WIRED*, March 29, 2023, https://www.wired.com/story/tiktok-hearing-congress-us-privacy-law/.

38 "Energy and Commerce to Bring TikTok CEO Before Committee to Testify," Energy & Commerce Committee, March 16, 2023, https://energycommerce.house.gov/posts/energy-and-commerce-brings-tik-tok-ceo-before-committee-to-testify; "Re: Hearing Entitled 'TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms'," Energy & Commerce Committee, memo, March 20, 2013, https://d1dth6e84htgma.cloudfront.net/Memo_03_23_2023_Full_Committee_Tik_Tok_Hearing_55e129f043.pdf?updated_at=2023-03-20T21:12:05.159Z.

39 Kari Paul, "Trump's bid to ban TikTok and WeChat: where are we now?," *The Guardian*, September 29, 2020, https://www.theguardian.com/technology/2020/sep/29/trump-tiktok-wechat-china-us-explainer.

40 Bobby Allyn, "Biden Drops Trump's Ban on TikTok And WeChat — But Will Continue The Scrutiny," *npr*, June 9, 2021, https://www.npr.org/2021/06/09/1004750274/biden-replaces-trump-bans-on-tiktok-wechat-with-order-to-scrutinize-apps.

41 David McCabe and Cecilia Kang, "U.S. Pushes for TikTok Sale to Resolve National Security Concerns," *The New York Times*, March 15, 2023, https://www.nytimes.com/2023/03/15/technology/tiktok-biden-pushes-sale.html; Jake Sullivan, "Statement from National Security Advisor Jake Sullivan on the Introduction of the RESTRICT Act," The White House, March 7, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/07/statement-from-national-security-advisor-jake-sullivan-on-the-introduction-of-the-restrict-act/.

42 Alyssa Newcomb, "A timeline of Facebook's privacy issues — and its responses," *NBC News*, March 24, 2018, https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651.

43 Newcomb, "A timeline of Facebook's privacy issues."

44 Nicholas Confessore and Cecilia Kang, "Facebook Data Scandals Stoke Criticism That a Privacy Watchdog Too Rarely Bites," *The New York Times*, December 30, 2018, https://www.nytimes.com/2018/12/30/technology/facebook-data-privacy-ftc.html.

45 Salvador Rodriguez, "Senators demand Facebook CEO Mark Zuckerberg answer questions after whistleblower's revelations at hearing," *CNBC*, October 5, 2021, https://www.cnbc.com/2021/10/05/congress-demands-mark-zuckerberg-answer-questions-at-haugen-hearing.html.

46 "California Consumer Privacy Act (CCPA)," Office of the California Attorney General, accessed May 30, 2023, https://oag.ca.gov/privacy/ccpa.

47 Todd Feathers, "Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious," *The Markup*, April 15, 2021, https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious.

48 Feathers, "Big Tech Is Pushing States to Pass Privacy Laws; Diane Bartz, "U.S. bill to rein in Big Tech backed by dozens of small and big companies," *Reuters*, June 13, 2022, https://www.reuters.com/technology/dozens-companies-small-business-groups-back-us-bill-rein-big-tech-2022-06-13/.

49 "Governor Newsom, Attorney General Bonta and CPPA File Letter Opposing Federal Privacy Preemption," Office of Governor Gavin Newsom, February 28, 2023, https://www.gov.ca.gov/2023/02/28/governor-newsom-attorney-general-bonta-and-cppa-file-letter-opposing-federal-privacy-preemption/.

50 Rob Bonta, Letter to Congressional Leaders, July 19, 2022, https://oag.ca.gov/system/files/attachments/press-docs/Letter%20to%20Congress%20re%20Federal%20Privacy.pdf.

51 Sullivan, "Statement from National Security Advisor Jake Sullivan on the Introduction of the RESTRICT Act."

52 Sullivan, "Statement from National Security Advisor Jake Sullivan on the Introduction of the RESTRICT Act"; "Senators Introduce Bipartisan Bill to Tackle National Security Threats from Foreign Tech," Office of U.S. Senator Mark R. Warner, March 7, 2023, https://www.warner.senate.gov/public/index.cfm/2023/3/senators-introduce-bipartisan-bill-to-tackle-national-security-threats-from-foreign-tech.

53 "Manchin, Bipartisan Colleagues Introduce Restrict Act to Protect Americans Online, Defend National Security From Foreign Technology," Office of U.S. Senator Joe Manchin, March 7, 2023, https://www.manchin.senate.gov/newsroom/press-releases/manchin-bipartisan-colleagues-introduce-restrict-act-to-protect-americans-online-defend-national-security-from-foreign-technology.

54 U.S. President Donald Trump, "Securing the Information and Communications Technology and Services Supply Chain," Executive Order 13873, May 15, 2019, https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

55 Department of the Treasury, Office of Investment Security, "Provisions Pertaining to Certain Investments in the United States by Foreign Persons," 31 CFR Parts 800 and 801, RIN 1505–AC64, January 17, 2020, https://home.treasury.gov/system/files/206/Part-800-Final-Rule-Jan-17-2020.pdf.

56 "The American Data Privacy and Protection Act," American Bar Association, August 30, 2022, https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/august-22-wl/data-privacy-0822wl/.

57 "The American Data Privacy and Protection Act," American Bar Association.

58 Biden, "Republicans and Democrats, Unite Against Big Tech Abuses."

59 "Innovation, Data, and Commerce Subcommittee Hearing: 'Economic Danger Zone: How America Competes to Win the Future Versus China'," hearing in front of the U.S. House Energy & Commerce Committee, February 1, 2023, https://energycommerce.house.gov/events/innovation-data-and-commerce-hearing-is-entitled-economic-danger-zone-how-america-competes-to-win-the-future-versus-china; "Innovation, Data, and Commerce Subcommittee Hearing: 'Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy'," hearing in front of the U.S. House Energy & Commerce Committee, March 1, 2023, https://energycommerce.house.gov/events/innovation-data-and-commerce-subcommittee-hearing-promoting-u-s-innovation-and-individual-liberty-through-a-national-standard-for-data-privacy.

60 "'Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy'," hearing in front of the U.S. House Energy & Commerce Committee.

61 "Bipartisan E&C Leaders Hail Committee Passage of the American Data Privacy and Protection Act," Energy & Commerce Committee, July 20, 2022, https://energycommerce.house.gov/posts/bipartisan-ec-leaders-hail-committee-passage-of-the-american-data-privacy-and-protection-act.

62 Zeran v. America Online, Inc., 958 F. Supp. 1124 (E.D. Va. 1997).

63 Ron Wyden, "I wrote this law to protect free speech. Now Trump wants to revoke it," *CNN Business*, June 9, 2020, https://www.cnn.com/2020/06/09/perspectives/ron-wyden-section-230/index.html.

64 Biden, "Republicans and Democrats, Unite Against Big Tech Abuses."

65 U.S. Congress, Senate, *A bill to amend the Internal Revenue Code of 1986 to increase the additional 2020 recovery rebates, to repeal section 230 of the Communications Act of 1934, and for other purposes*, S.5085, introduced in Senate December 29, 2020, https://www.congress.gov/bill/116th-congress/senate-bill/5085; U.S. Congress, House, SAFE TECH Act, H.R. 1231, introduced in House February 28, 2023, https://www.congress.gov/bill/118th-congress/house-bill/1231.

66 "Re: Hearing Entitled 'TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms'," Energy & Commerce Committee.

67 Catherine Thorbecke, "Montana's TikTok ban leaves users, business owners reeling," *CNN*, May 21, 2023, https://www.cnn.com/2023/05/21/tech/montana-tiktok-users/index.html; Lisa Marie Basile, "Here's why a TikTok ban could affect both physicians and their patients," *MD Linx*, March 31, 2023, https://www.mdlinx.com/article/heres-why-a-tiktok-ban-could-affect-both-physicians-and-their-patients/nZThoSe6j8nDrJ4NrtxcJ; Haleluya Hadero, "Montana is banning TikTok. But can the state enforce the law and fend off lawsuits?," *AP News*, May 22, 2023, https://apnews.com/article/tiktok-ban-montana-china-data-chinese-government-71143a3a87c9a0b692d927f72b6fec70.

68 Biden, "Republicans and Democrats, Unite Against Big Tech Abuses."

The Institute for China-America Studies (ICAS) is an independent think tank in Washington D.C. ICAS focuses on the evolving dynamics in the U.S.-China relationship to promote greater collaboration and mutual understanding through sincere exchanges of fresh ideas, objective policy-oriented research, and fair assessments of this critical bilateral relationship.

We aim to provide a window into the worldviews of both the United States and China, and thereby serve as a vehicle to promote greater understanding between these two countries and societies.

ICAS
Institute for China-America Studies

1919 M St. NW, Suite 310
Washington, DC 20036
(202) 968-0595 | www.chinaus-icas.org