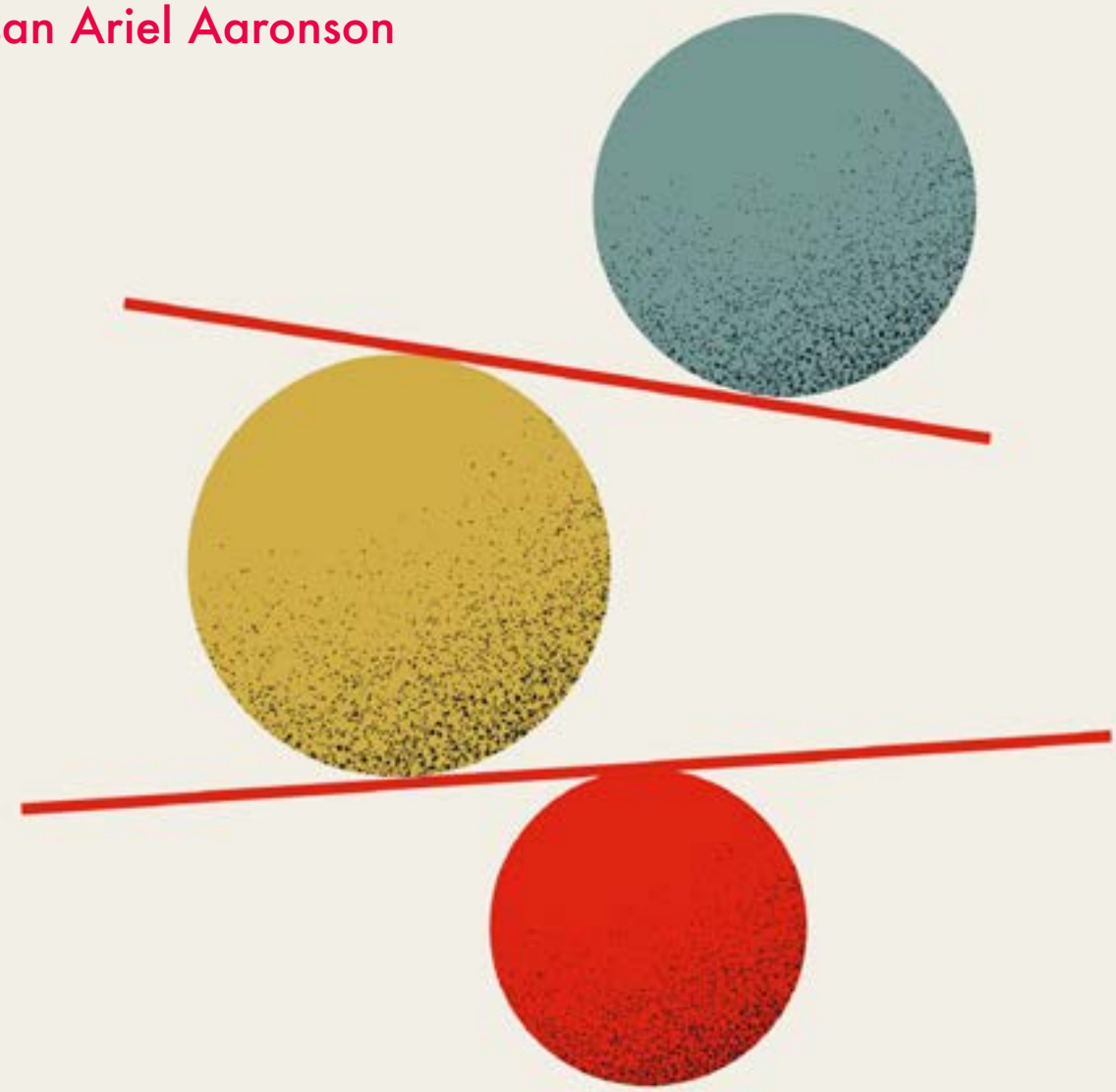
Centre for International
Governance Innovation

CIGI Papers No. 330 – August 2025

# A Difficult Balance

## Privacy, National Security and the Free Flow of Data

Susan Ariel Aaronson



Centre for International
Governance Innovation

CIGI Papers No. 330 — August 2025

# A Difficult Balance

## Privacy, National Security and the Free Flow of Data

Susan Ariel Aaronson

## About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

## À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

## Credits

**Research Director, Digital Economy** S. Yash Kalash
**Director, Program Management** Dianna English
**Program Manager** Jenny Thiel
**Publications Editor** Susan Bubak
**Publications Editor** Christine Robertson
**Graphic Designer** Sepideh Shomali



67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

# Table of Contents

## About the Author

Susan Ariel Aaronson is a CIGI senior fellow, research professor of international affairs at George Washington University (GWU) and co-principal investigator with the NSF-NIST Institute for Trustworthy AI in Law & Society, where she leads research on data and AI governance. She is also a GWU Public Interest Technology Scholar and a Balsillie Tech Scholar. Her research interests relate to the relationship between economic change, human rights and good governance.

Susan directs the Digital Trade and Data Governance Hub at GWU. The Hub was founded in 2019 and educates policy makers, the press and the public about data governance and data-driven change through conferences, webinars, study groups, primers and scholarly papers. It is the only organization in the world that maps the governance of public, proprietary and personal data at the domestic and international levels. The Hub's research has been funded by foundations such as Ford and Minderoo.

Susan directs projects on responsible AI, AI and trade and AI overcapacity, as well as a new metric for data governance. She regularly writes op-eds for *Barron's*, *Fortune* and other publications, and has been a commentor on economics for NPR's *Marketplace*, *All Things Considered* and *Morning Edition*, and for NBC, CNN, the BBC and PBS.

Previously, Susan was a guest scholar in economics at the Brookings Institution (1995–1999) and a research fellow at the World Trade Institute (2008–2012). Susan was also the Carvalho Fellow at the Government Accountability Project and held the Minerva Chair at the National War College. She has served on the business and human rights advisory board at Amnesty International and the advisory board of Human Rights under Pressure, a joint German and Israeli initiative on human rights.

In her spare time, Susan enjoys triathlons and ballet.

## Acronyms and Abbreviations

| | |
|---|---|
| AFL-CIO | American Federation of Labor and Congress of Industrial Organizations |
| AI | artificial intelligence |
| APEC | Asia-Pacific Economic Cooperation |
| CBPR | Cross-Border Privacy Rules |
| DFFT | data free flow with trust |
| FTA | free trade agreement |
| FTC | Federal Trade Commission |
| G7 | Group of Seven |
| ICT | information and communications technology |
| IP | intellectual property |
| IPEF | Indo-Pacific Economic Forum |
| IT | information technology |
| JSI | Joint Statement Initiative |
| NAFTA | North American Free Trade Agreement |
| OECD | Organisation for Economic Co-operation and Development |
| PADFA | Protecting Americans' Data from Foreign Adversaries Act |
| TPP | Trans-Pacific Partnership |
| TTIP | Transatlantic Trade and Investment Partnership |
| USMCA | United States-Mexico-Canada Agreement |
| USTR | United States Trade Representative |
| WTO | World Trade Organization |

# Executive Summary

Since the 1970s, the US government has led efforts to open data and to encourage data flows. It has also called for shared rules and clear exceptions to govern the free flow of data in trade agreements. Given that history, in October 2023, the Biden administration shocked many of its trade partners when it announced that it would end its support for proposals to encourage the free flow of data across borders being discussed in the World Trade Organization (WTO). Policy makers said they wanted to assess whether supporting these proposals remained in the US national interest. Soon thereafter, the United States established restrictions on the sale and transfer of various types of data to China and several other adversary nations. The United States acted on its own, through executive orders, rather than trying to get internationally approved language in trade agreements. This paper attempts to explain how and why the United States became more concerned about the national security risks of the free flow of data across borders. Moreover, the author examines the implications of such restrictions on data, access to data and the quality of data.

US President Joe Biden (2020–2024) was not the first president to enact some restrictions on cross-border data flows through executive orders. But earlier restrictions were more limited, and from the 1980s until 2024, the United States tried to work with other countries on minimizing such restrictions. However, restrictions on the free flow of data are likely more consequential today, as data underpins the US and global economy. The Trump administration has not only continued Biden-era restrictions but has also limited access to US government data sources and even stopped collecting and posting data. Such actions could alienate other countries and make America's data-driven sectors less competitive.

The author argues that in the age of generative AI, policy makers need a more comprehensive analysis of the costs and benefits of openness and the free flow of data.[1] By making such an assessment, governments such as Canada and the United States will be better positioned to ensure that individuals and governments — and not just corporations — can control and capture the value of data.

# Introduction

Times and technologies change, people change and national positions evolve. Although change is inevitable, and can be gradual or radical, many people find change jarring. America's evolving position on the free flow of data provides a good example because it looked like the world's leader of efforts to encourage the free flow and utilization of data was advocating for greater restrictions on openness. This paper examines how and why this occurred.

To some degree, America's rising restrictions on data are understandable. After all, data has never been totally benign. Throughout history, some individuals have threatened to reveal private information to prod another person to change their behaviour. Moreover, some countries have historically used disinformation to undermine trust and societal cohesiveness in other countries (Posetti and Matthews 2018; Lanoszka 2019; Lucas 2019).

Since the 1970s, US officials have advocated for rules governing the free flow of data within trade agreements. They believed that such rules supported democracy, innovation and economic growth — all long-standing US priorities. At the same time, these officials acknowledged that there must be exceptions to any such rules. Bad actors might hack, steal and/or misuse data sets to manipulate individuals and groups; undermine their human rights; and/or expose personal information that individuals may want to keep private. Thus, US policy makers thought they could establish clear rules, making the free flow of data a default while using trade agreement exceptions when officials needed to limit such flows to protect national security, public morals or privacy (Drake 1993, 278–81, 82).

But the balance favouring the free flow of data began to change during the Trump administration. In May 2019, US President Donald Trump (January 2017 to January 2021) issued an executive order to make it harder for foreign adversaries to

1 This paper is based on work supported, in part, by the NSF-NIST Institute for Trustworthy AI in Law and Society, which is supported by the National Science Foundation under award 2229885. Any opinion, finding and conclusion or recommendation expressed herein represents that of the author and does not necessarily reflect the views of the NSF.

exploit vulnerabilities in the information and communications technology (ICT) supply chain and to protect sensitive information stored in and communicated through ICT products and services.[2]

President Biden made the most dramatic changes to this balancing act, acting at the national and international levels. First, on June 9, 2021, he issued an executive order requiring the Secretary of Commerce to "evaluate on a continuing basis transactions involving connected software applications that may pose an undue risk of sabotage or subversion of... information and communications technology or services in the United States; pose an undue risk of catastrophic effects on the security or resiliency of the critical infrastructure or digital economy of the United States; or otherwise pose an unacceptable risk to the national security of the United States or the security and safety of United States persons."[3] In April 2024, Congress passed, and the president signed, the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFA), which prohibits data brokerage transactions with foreign adversaries related to US citizens' personally identifiable sensitive data.[4] In December 2024, the US Department of Justice issued a final rule designed to restrict the sale of personal data to China, Iran, North Korea and Russia.[5] US officials feared (and continue to fear) that China and other adversaries could mix such data with other data sets and/or, perhaps ominously, use sophisticated data analytics to make predictions about or to manipulate US citizens (Corey 2024; Aaronson 2020).

The Biden administration did not only use domestic policies to govern cross-border data flows. In contrast with the Bush, Obama and Trump administrations before it, the Biden administration signed no new trade agreements related to the free flow of information or data.[6] Instead, as noted above, it created alternative frameworks to trade agreements to govern data. First, in 2022, it announced, negotiated and then partially abandoned a regional framework and forum that would include provisions on digital trade — the Indo-Pacific Economic Forum (IPEF). The IPEF had a trade pillar that addressed cross-border data flows.[7] Second, in 2022, it set up the Global Cross-Border Privacy Rules (CBPR) Forum with Australia, Canada, Chinese Taipei, Japan, Mexico, the Philippines, the Republic of Korea and Singapore. The CBPR Forum uses voluntary discussions and certifications to enable the free flow of data, including personal data.[8]

Finally, the Biden administration seemed to reverse decades of US efforts to include rules governing the free flow of data across borders in trade agreements. In late October 2023, trade journalists reported that "the Biden administration will end its support for proposals on data flows, data localization and source code being discussed in [the] World Trade Organization" and assess if supporting these proposals remained in the US national interest (Dupont 2023; Reuters 2024; Lester 2023).

The Biden policies were misreported; it was not abandoning the Joint Statement Initiative (JSI) at the WTO. In a press release, the Office of the US Trade Representative (USTR) stated, "Many countries, including the United States, are examining their approaches to data and source

2 *Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed Reg 22689 (2019), online: <www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain>.

3 *Protecting Americans' Sensitive Data From Foreign Adversaries*, 86 Fed Reg 31423 (2021) at 31425 [*Protecting Americans*], online: <www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries>.

4 US, Bill HR 815, *Making emergency supplemental appropriations for the fiscal year ending September 30, 2024, and for other purposes*, 118th Cong, 2024 (enacted), online: <www.congress.gov/bill/118th-congress/house-bill/815> [*Emergency supplemental appropriations*] (this bill was designed to provide supplemental assistance for foreign policy and defence purposes).

5 The "final rule" identifies countries of concern and covered persons to whom the final rule applies, and designates classes of prohibited, restricted and exempt transactions. The final rule establishes bulk thresholds for certain types of sensitive personal data, including human genomic data, biometric identifiers, precise geolocation data, personal health data, personal financial data and certain covered personal identifiers. The final rule also prescribes processes to obtain licences authorizing otherwise prohibited or restricted transactions; develops protocols for the designation of covered persons; and provides advisory opinions, and recordkeeping, reporting and other due diligence obligations for covered transactions. See US Department of Justice (2024).

6 See https://ustr.gov/issue-areas/services-investment/telecom-e-commerce/e-commerce-fta-chapters; https://ustr.gov/issue-areas/services-investment/ict-services-and-digital-trade/digital-trade-fact-sheets. The fact sheets were not updated during the Biden administration. The Trump administration agreed to two digital trade chapters with Japan and in the United States-Mexico-Canada Agreement (USMCA or the North American Free Trade Agreement [NAFTA] 2.0).

7 See www.commerce.gov/ipef; www.commerce.gov/ipef/pillar-iFair Economy.

8 See www.globalcbpr.org/about/.

code, and the impact of trade rules in these areas. In order to provide enough policy space for those debates to unfold, the United States has removed its support for proposals that might prejudice or hinder those domestic policy considerations. The JSI continues to be an important initiative and the United States intends to remain an active participant in those talks" (USTR 2023).

Nonetheless, some observers saw these actions as a significant policy change, undermining US credibility as an advocate for openness (Broadbent 2023). *The Wall Street Journal* Editorial Board (2023) suggested that Biden just gave a huge gift to China. Thirty-two senators wrote a letter asking President Biden to reverse the decision and reaffirm America's global economic leadership "that China and Russia will fill" (Cassidy 2023). Human rights proponents argued that without US support for these provisions, "the internet will further fracture, authoritarians will be emboldened, and human rights advocates could suffer" (Funk and Brody 2023, 2024). A senior official at the International Association for Privacy Professionals described this situation as the beginning of the end of the free flow of data (Zweifel-Keegan 2024).

The Biden administration's actions could also affect the US and global economy because even limited restrictions could have economic and societal costs (Bella and Sarin 2023). Services are essential to US economic health and underpin US manufacturing (Calderon and Rasser 2022; Trachtenberg 2024). In 2024, the White House noted that digitally enabled services drive the US economy and the US services export surplus. Digitally enabled services represent the fastest-growing segment in trade, underpinned by data flows and analysis (The White House 2024a; Baldwin 2022). Moreover, these restrictions could affect the accuracy of US data-driven technologies, such as artificial intelligence (AI), because developers need the most accurate, complete and representative data sets to create AI that does not make mistakes or make up information (WTO 2024a). But it is important to note that the United States is not alone in increasing such restrictions on data (Gonzalez et al. 2025).

This paper relies on primary source data and uses process tracing to answer two questions:

- How and why did US policy makers gradually change how the US government regulated cross-border data flows?
- What are the implications of this new vision of data for the US and global economy? The Trump administration has not commented on or altered these policies.

This paper proceeds as follows: the author begins with the definitions of terms related to information and data (see Box 1). Next, the author delineates why the free flow of information is important and then traces the history of US efforts to encourage such flows. The author also details recent US efforts to limit such flows. Next, the author attempts to explain the multiple factors that have driven US policy makers to make these changes. Finally, the author discusses the implications of this dramatic policy change and what it means for US leadership of the global economy as well as leadership in data-driven technology.

The author notes five important caveats.

- In general, the writing does not distinguish among various types of data (proprietary, personal and public data) unless US positions, laws or regulations make such distinctions. The paper focuses on how the failure to protect personal data and the accumulation of large troves of data by market actors worldwide raise national security risks for the United States.
- Although data and information are not the same, policy makers around the world often use the terms interchangeably when they are discussing data flows among countries. Hence, this paper will do so as well when talking about data flows. The United States used "data flows" in digital trade chapters (Drake 1993; Aaronson and Struett 2020). However, many of the most recent US trade agreements use "information flows" (Organisation for Economic Co-operation and Development [OECD] 2015). In the recent EU-Singapore digital trade agreement, the European Union uses "data flows."[9] The JSI being negotiated by more than 90 WTO members does not have agreed provisions on cross-border data flows, but article 25 discusses cross-border

9 See, as example, *Agreement on Digital Trade between the European Union and the Republic of Singapore*, 20 July 2023, arts 5, 6 (entered into force 25 July 2024), online: <https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/66ccfa9f-e239-4893-8e12-64f8ff1d1221/details?download=true>. It does not mention information flows.

data transfers.[10] In contrast, recent Pacific trade agreements, such as the Digital Economy Partnership Agreement and the Regional Comprehensive Economic Partnership, use "information flows," although they often talk about data, such as open data or personal data, as well (Leblond 2024).

- The author acknowledges a bias that data flows and data sharing among societies, sectors and institutions are good for the world, and that some types of data can be considered global public goods (United Nations Conference on Trade and Development 2021, 198). At the same time, the author notes that personal and intellectual property (IP) data could create risks to individuals and the nation without proper protection (Aaronson 2020; Ryan and Christl 2023).
- The paper only covers through the Biden administration and the first four months of the Trump administration (January–April 2025). The Trump administration has not yet clarified its position on the free flow of data. But it is important to note that the Trump administration has stopped collecting and displaying many official troves of data related to diversity, climate, health care and other topics (MacGillis 2025).[11] These data troves are essential to enable US government stakeholders to evaluate government policies and programs; they are also likely to be useful for AI. Such data is essential to public policy evaluation but also for AI.
- Finally, the author does not address investment restrictions — another tool the United States is using to limit cross-border information flows.

## Box 1: Definitions of Terms

**Data** can be defined as the representation of facts stored or transmitted as qualified or quantified symbols. One can use data to develop information and, ultimately, knowledge.

**Information** can be defined as the meaning resulting from the interpretation of facts as conveyed through data or other sources such as words. Hence, data is a subset of information. Information is the lifeblood of a robust democracy and productive economy.

**Privacy** is protected through strategies that govern the collection, use and dissemination of personal information.

**Data security** is enforced through strategies to protect personal information from unauthorized access or use and respond to such unauthorized access or use.

**Datafication** refers to the process by which subjects, objects and practices are transformed into digital data (Southerton 2020).

**Digital trade** includes a wide range of activities facilitated by digital technologies, including the exchange of data and services.

**E-commerce** specifically refers to the buying and selling of goods and services online through digital platforms, such as websites or marketplaces; essentially, e-commerce is a subset of digital trade. However, the terms "e-commerce" and "digital trade" are often used interchangeably (Alschner 2023).

**Data free flow with trust (DFFT)** refers to a strategy promulgated by the Government of Japan and later adopted by members of the OECD to promote the free flow of data while simultaneously ensuring trust in privacy, security and IP rights. In 2023, Group of Seven (G7) leaders endorsed the G7 Digital and Tech Ministers' "Vision for Operationalising DFFT and Its Priorities." Soon thereafter, the OECD created a committee of experts to find ways to operationalize DFFT.

10 WTO, *Joint Statement Initiative on Electronic Commerce*, WTO Doc INF/ECOM/87 (2024), art 16.3 [*JSI*].

11 See www.datarescueproject.org/ and Natanson (2025).

# Why Should People Care About the Evolving US Position on the Free Flow of Data?

Below, the author provides some reasons why the changing US position on the free flow of data is important.

- **The United States is particularly dependent on global data flows, which fuel its data-driven economy.** The White House notes that digitally enabled services represent the fastest-growing segment of global trade, far outpacing other goods and services exports (Baldwin 2022). This trend comports with the expansion of the US digital economy — economic activity generated from or supporting electronic connections. In 2022, while US real GDP grew by 1.9 percent, the US digital economy real value added grew by 6.3 percent — driven primarily by growth in software and telecommunication services (The White House 2024b).
- **The United States and other countries benefit from rules governing data.** Clear, internationally accepted rules governing cross-border data flows are important to economic growth, human welfare, democratic governance and technological development. In 1946, UN member states decreed in the Universal Declaration of Human Rights that access to information (often called freedom of information) is not only a fundamental human right that governments must respect but also "the touchstone of all the freedoms to which the United Nations is consecrated" (Mendel, n.d.). Countries that work to provide information about their actions and policies facilitate democracy, encourage economic growth and work toward good governance. Access to information allows citizens to guide policy makers and hold them to account, and it facilitates open debate among researchers (Berliner 2014; Florini 1998). Citizens, countries and firms also benefit when there are clear rules governing data flows across borders. However, the UN member states also agreed that there would be times when states may need to restrict access to information in order to protect the rights or reputations of others, national security and public order, and public health or morals.[12] Trade agreements include similar exceptions, although policy makers do not really know when they can take such exceptions because they have not been sufficiently clarified through trade disputes.
- **There is growing evidence that data flow provisions can both facilitate and hinder trade** (López González, Del Giovane and Ferencz 2025; Aaronson 2024). Scholars are also finding that barriers to digital trade increase costs to firms and result in less trade (Aaronson 2019; Reichman and Maskus 2004). A recent study examined the implications of data flow restrictions on global GDP and trade and found that if all economies fully restricted their data flows, it could result in a five percent reduction in global GDP and a 10 percent decrease in exports. However, the study also found that restrictive measures to protect personal data help build trust in data-driven technologies such as AI and digital trade (OECD and WTO 2025).

As the next section illustrates, US support for the free flow of information was a constant from the 1970s to 2019. But the rise in hacking and misuse of various types of data, as well as the centrality of data for AI, led some policy makers to rethink their views about the benefits of the collection, monetization, sales and flows of data across borders. As noted above, large troves of data could be dangerous to individuals and the nation's security.

# The Evolution of US Policies Regarding Cross-Border Data Flows

For much of the twentieth century, open data and the free flow of information seemed to enhance human welfare and agency. New technologies

12 The limitations on freedom of expression are spelled out in the *International Covenant on Civil and Political Rights,* 16 December 1966, GA Res 2200A(XXI), art 19(3) (entered into force 23 March 1976), online: <www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>. See www.article19.org/pages/en/limitations.html; https://tinyurl.com/4rnyjwcb.

## Box 2: Some Facts About Data and Datafication

Data has never been totally benign. Throughout history, some individuals have threatened to reveal private information to prod another person to change their behaviour. Moreover, some countries have historically used disinformation to undermine trust and societal cohesiveness (Lucas 2019).

Data begets ever more data. When you text, you produce data that is content, but the texting platform also receives data about when, where and with whom you texted. When you use an app, firms may ask for a wide range of your data sets such as your contact lists. All of these data types are a form of metadata that firms or governments can use to make predictions or other forms of analysis (Rashid 2014).

provided additional means for people to connect, learn and broadcast (Van Dijck 2020). But the data-driven economy did not always yield a virtuous circle. In the 1970s, information became a commodity that could be sold for current or future use (Drake 1993; OECD 2022). In the next decades, many public and private entities began to ask their stakeholders (workers, suppliers and customers) for more and more data as they provided services online (datafication). These individuals and their national policy makers struggled to protect individual privacy. Meanwhile, many firms adopted a new business model — one that fuelled extensive cross-border data flows over the internet. Many companies provide free services to their users in return for the use of their personal data. Their users rely on computer and mobile phone applications that collect data about their activities and movements. These same firms began to use the large troves of personal information they collected to predict the behaviour of individuals and groups and to influence and modify that behaviour (see Box 2). They also began to sell their data and predictions to other firms, governments and entities. Today, this practice is called "surveillance capitalism" (Zuboff 2019).

Gradually and collectively, these business practices created problems for individuals as well as for policy makers. While large troves of personal data became an important asset for the entities that collected data, they also present risk. Bad actors can steal, manipulate or hack these troves of data. Moreover, such data, even when anonymized, can reveal information about large groups of people and even a government's objectives and strategies. Thus, governments are also vulnerable when personal data held by governments or firms can be hacked or stolen and then compiled, analyzed and even monetized (Aaronson 2020; Government Accountability Office 2024; National Intelligence Council 2021, 59). US public and private entities are especially vulnerable to the risks of cybertheft or cyber manipulation because the United States lacks a national law delineating how firms can collect, analyze, utilize and sell personal data, although the country has strong sector-specific laws. Members of Congress have yet to agree on the conceptual framework of the law (i.e., whether it is prescriptive or outcome-based); the scope of the law and its definition of protected information; and the role of the Federal Trade Commission (FTC) (which protects consumers) or another federal enforcement agency. Congress also has no consensus on which entities are liable and how injured consumers might find remedies in court (Mulligan and Linebaugh 2022). In addition, Congress has not agreed on rules governing the behaviour of data brokers — market actors that sell and distribute troves of personal data. The United States, in short, has a major gap in data governance.

Despite that gap in its own data governance, the United States has long pushed for other countries to develop a system of shared governance for cross-border data flows. The United States was — and remains — the world's leading supplier of information services such as software, movies, and financial and telecommunications services. In 1986, US trade policy makers called for rules governing such services within the Uruguay Round of multilateral trade talks. But officials from other nations feared that the delineation of such rules could undermine their sovereignty and their ability to restrict cross-border data flows to protect personal data, privacy, national security, culture and public morals. For example, Canada

and France were among several important US trade partners that balked at establishing such rules in trade agreements rather than within other UN bodies (Drake 1993; Drake and Nicolaïdis 2000). Some opponents seized on a Canadian argument that transborder data flows were a threat to "information sovereignty" — the ability to control what information flowed into or out of a country's borders. In addition, officials from many developing countries worried that they could become information poor and lose control over locally developed information (Aaronson 2016).[13]

Moreover, critics could easily point to what they saw as the inconsistency of the US position. On one hand, President Ronald Reagan issued a national security decision directive that limited foreign access to classified "fundamental research" in science, technology and engineering in 1984.[14] The Reagan administration was concerned that the Soviet Union and its allies could acquire US expertise in technologies. The directive was very clear that only classified scientific or technological information would be restricted and only for those nations.[15] On the other hand, when he visited London, England, in 1989, he called information "the oxygen of the modern age" and noted that governments (including the United States) could not suppress it (Rule 1989).

Trade negotiators were not able to find common ground on language encouraging the free flow of data in this period. Policy makers around the world recognized that they needed to facilitate these flows, but they did not agree on how, when and where data flows could be restricted (National Research Council 1987, 24–27; Drake 1993). Meanwhile, US companies and researchers continued to dominate the computer and software markets.[16]

With the advent of the commercial internet, from 1997 to 2017, the United States again led efforts to set rules governing data at the bilateral, regional and multilateral levels. In 1997, the Clinton administration issued the Framework for Global Electronic Commerce, which provided a road map for international negotiations on data. It states, "The U.S. government supports the broadest possible free flow of information across international borders….The Administration…will develop an informal dialogue with key trading partners…to ensure that differences in national regulation… do not serve as disguised trade barriers."[17]

During the Clinton administration (1992–2000), the United States signed bilateral agreements with France, Ireland, Japan, the Netherlands and South Korea, in which the signatories agreed to remove barriers to e-commerce. But these agreements did not address differences in legal approaches to privacy. In 1998, the OECD issued principles to guide policy makers in protecting privacy.[18] The Secretariat explained that "when individuals have confidence in the protections surrounding their personal data, they are more likely to engage in online activities, share information, and participate in the digital economy."[19] According to the OECD, privacy drives trust online, which, in turn, will yield economic growth, foster innovation and encourage the free flow of data across borders. But in the twentieth century, nations were unable to find common ground on how to encourage cross-border data flows and protect national security, public morals and other important policy goals. They continued to try in the twenty-first century.[20]

In 2003, Australia and Singapore became the first countries to agree to binding language delineating the free flow of data. The financial services chapter of their trade agreement states that "neither Party shall take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means….Nothing in this Article restricts the right of a Party to

13 California, Oregon, Texas and Vermont enacted data broker regulations (Davis+Gilbert 2023); also see Wugmeister, Folio and Martinez (2024); Pozza et al. (2024); Brown, Chin-Rothmann and Brock (2024).

14 National Security Decision Directive 189, *National Policy on the Transfer of Scientific, Technical and Engineering Information,* 21 September 1985, online: <https://irp.fas.org/offdocs/nsdd/index.html>.

15 Ibid.

16 See https://en.wikipedia.org/wiki/Timeline_of_computing_1980%E2%80%931989.

17 See https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html.

18 These build on earlier recommendations for privacy guidelines. See OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,* 23 September 1980, OECD/LEGAL/0188, online: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>.

19 See www.oecd.org/en/topics/policy-issues/privacy-and-data-protection.html.

20 For a comparison of approaches to cross-border data flows, see https://globaldataalliance.org/wp-content/uploads/2023/02/02082023gdaexplanatorytable.pdf. For analysis, see Aaronson and Struett (2020) and Burri, Vásquez Callo-Müller and Kugler (2024).

protect personal data, personal privacy and the confidentiality of individual records and accounts…so long as such right is not used to circumvent the provisions of this Chapter."[21]

Soon thereafter, during the Bush administration (January 2001–January 2009), the USTR negotiated for the United States to become a party to e-commerce chapters in bilateral trade agreements with Australia, Bahrain and several other nations. These agreements set parameters for the sale and exchange of goods and services online. However, these agreements did not mention data or information flows.[22] Meanwhile, the Bush administration also made achievement of a multilateral agreement a trade policy priority. In 1998, WTO ministers adopted a declaration on global e-commerce that called on the WTO to establish a comprehensive work program on e-commerce. The Work Programme on Electronic Commerce defined e-commerce broadly as "the production, distribution, marketing, sale or delivery of goods and services by electronic means."[23] Here, too, the declaration said nothing specific about data flows, but it was flexible enough to include an ever-growing panoply of goods and services built on data, such as AI or apps (Aaronson and Struett 2020).

Meanwhile, during the Obama administration (January 2009–January 2017), policy makers moved to make public data more open and available by making it machine readable, which means it could be easily computerized and shared. Officials asserted that "making information resources easy to find, accessible, and usable can fuel entrepreneurship, innovation, and scientific discovery that improves Americans' lives and contributes significantly to job creation" (The White House 2013). However, the order also reflected national security concerns: "Nothing in this order shall compel or authorize the disclosure of privileged information, law enforcement information, national security information, personal information, or information the disclosure of which is prohibited by law" (ibid.).

In 2012, the United States and the Republic of Korea became the first nations to include non-binding language related to the free flow of information in the electronic commerce chapter of their free trade agreement (FTA). Article 15.8 states that "the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[24] The agreement also included language on personal data protection. But rather than encouraging interoperability of privacy regimes, the language stated that each party "shall adopt or maintain a legal framework that provides for the protection of the personal data of users of electronic commerce." The United States could only agree to this vague language because the country lacked a national and unified rather than sector-specific data protection law (Monteiro and Teh 2017).

After the US-Korea FTA, the Obama administration decided to make the language in its future agreements binding (*countries must or shall do x* instead of *countries shall endeavour to do x*) and disputable (one state may challenge another country's policies as trade distorting) (Aaronson 2016). By 2017, the United States had 11 digital trade agreements with 16 countries (but most of these were negotiated before the binding free flow language).[25]

However, the Obama presidency did not yield international agreements that clarified when data could flow freely and when and how nations could restrict those flows. It was not for lack of trying. The Obama administration wanted to develop broader agreements that would include more countries and could serve as templates for a future international agreement under the WTO. Obama-era trade officials began to negotiate two important agreements — one with Pacific-facing nations

21 *Indonesia-Australia Comprehensive Economic Partnership Agreement*, 4 March 2019, c 10, art 10.4 (entered into force 5 July 2020), online: <www.dfat.gov.au/trade/agreements/in-force/iacepa/iacepa-text/Pages/iacepa-chapter-10-financial-services>; *Singapore-Australia Free Trade Agreement*, 17 February 2003, c 9, c 14, art 4 (entered into force 28 July 2003), online: <www.austlii.edu.au/au/other/dfat/treaties/2003/16.html#art14>.

22 See, as example, *United States-Australia Free Trade Agreement*, 18 May 2004, c 16 (entered into force 1 January 2005) or *United States-Bahrain Free Trade Agreement*, 14 September 2004, c 13 (11 January 2006) (both chapters can be found at https://ustr.gov/issue-areas/services-investment/telecom-e-commerce/e-commerce-fta-chapters).

23 See www.wto.org/english/tratop_e/ecom_e/ecom_work_programme_e.htm.

24 *United States-Korea Free Trade Agreement*, 30 June 2007, art 15.8 (entered into force 15 March 2012), online: <https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text>.

25 These countries included Australia, Bahrain, Chile, Colombia, Costa Rica, the Dominican Republic, El Salvador, Guatemala, Honduras, Japan, Morocco, Nicaragua, Oman, Panama and the Republic of Korea. See https://ustr.gov/issue-areas/services-investment/telecom-e-commerce/e-commerce-fta-chapters.

and one with Atlantic-facing nations. Obama administration officials wanted a counterweight to China's growing regional influence and so negotiated the 11-nation Trans-Pacific Partnership (TPP), which included a comprehensive digital trade chapter. This potential agreement was a foreign policy priority for the United States, as it hoped to bind 11 Pacific-facing nations in trade and, in so doing, counter the growing economic power of China. The TPP became an election issue that then candidate Trump vowed to oppose. As president, he abandoned the agreement in 2017 (USTR 2015, 2017a). The United States also tried to negotiate the Transatlantic Trade and Investment Partnership (TTIP), which would include a similar comprehensive digital trade chapter, with the 28-member state European Union. However, activists on both sides of the Atlantic saw the trade agreement as benefiting big business at the expense of the public. Given rising civil society anger, the participating governments agreed to abandon the TTIP talks (van Ham 2016; Dearden 2016).

In this period as well, Obama administration officials began to pay significant attention to barriers to the free flow of data. They began to list and describe these barriers and others in the annual Trade Agreements Program report to Congress and in fact sheets and other documents (USTR 2016a, 2016b, 2017b). For example, in explaining the language that the Obama administration negotiated in the TPP, the USTR noted, "Companies and consumers must be able to move data as they see fit. Many countries have enacted rules that put a chokehold on the free flow of information, which stifles competition and disadvantages American entrepreneurs. TPP combats these discriminatory and protectionist barriers with specific provisions designed to protect the movement of data, subject to reasonable safeguards like the protection of consumer data when exported" (USTR 2016a).

The Obama administration's focus on efforts to promote the free flow of data made economic sense, although these efforts were only partially successful. Many American businesses in the banking, entertainment and other sectors had long collected data about their stakeholders. Moreover, the United States was home to the biggest digital firms. All of those firms benefited from network effects — the ability to use their existing operations and data to create new technologies and greater exports — from AI to apps (United Nations Conference on Trade and Development 2021). These firms had significant influence over US policies. But other countries, including Australia, Canada, Mexico, the Phillipines and Singapore, also wanted to set clear, internationally accepted rules governing the free flow of data across borders (Aaronson and Struett 2020; United Nations Conference on Trade and Development 2021, 2023). These countries led and were active in efforts to set shared international rules at the WTO.

Despite its protectionist bent, the Trump administration (January 2017–January 2021) approved two agreements with provisions on digital trade. They updated the US-Japan FTA to include a digital trade chapter in 2019. They also added a digital trade chapter and other updates to NAFTA (now the USMCA). Moreover, the United States joined and collaborated with other nations at the WTO on the e-commerce JSI. Finally, the Trump administration also closely monitored and reported on barriers to US digital trade exports.[26]

Both the US-Japan FTA and USMCA contained binding language regarding the free flow of information: "No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person."[27] It then delineated exceptions: "This Article does not prevent a Party from adopting or maintaining a measure…that is necessary to achieve a legitimate public policy objective."[28] But the measure cannot be discriminatory or a disguised restriction on trade and does not impose restrictions on transfers of information greater than are necessary to achieve the objective.[29]

Trade policy makers also included language on open government data: USMCA article 19.18(1) states that "the Parties recognize that facilitating

26 For the Trump administration, see https://ustr.gov/issue-areas/services-investment/ict-services-and-digital-trade/digital-trade-fact-sheets and USTR (2019).

27 *United States-Mexico-Canada Agreement*, 30 November 2018, art 19.11(1) (entered into force 1 July 2020) [*USMCA*], online: <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement>.

28 Ibid, art 8.10(2).

29 A covered person or business must be domiciled in one of the signatories to the agreement. See *USMCA*, *supra note* 27, c 19, art 19.11; for the US-Japan FTA, see *Agreement between the United States of America and Japan Concerning Digital Trade*, 7 October 2019, art 11 (entered into force 1 January 2020) [*US-Japan Digital Trade Agreement*], online: <https://ustr.gov/countries-regions/japan-korea-apec/japan/us-japan-trade-agreement-negotiations/us-japan-digital-trade-agreement-text>.

public access to and use of government information fosters economic and social development, competitiveness, and innovation"[30]; article 19.18(2) states that "to the extent that a Party chooses to make government information, including data, available to the public, it shall endeavor to ensure that the information is in a machine-readable and open format and can be searched, retrieved, used, reused, and redistributed"[31]; and article 19.18(3) states that "the Parties shall endeavor to cooperate to identify ways in which each Party can expand access to and use of government information, including data, that the Party has made public, with a view to enhancing and generating business opportunities."[32] This language was neither binding nor disputable, but it set a norm that signalled that if policy makers wanted to incentivize data-driven sectors, providing public information that can be retrieved and reused was best practice.

Finally, both the US-Japan FTA and USMCA included a major change to the national security exception that could apply to cross-border data flows. Article 32.2(1) of the USMCA[33] and article 4 of the US-Japan Digital Trade Agreement[34] state that "nothing in this Agreement shall be construed to: (a) require a Party to furnish or allow access to information the disclosure of which it determines to be contrary to its essential security interests; or (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests." To some analysts, the United States sought a broader exception than that delineated in article XIV of the General Agreement on Tariffs and Trade (Ciuriak and Rodionova 2021). Kristina Irion, Margot E. Kaminski and Svetlana Yakovleva (2023) argue that this provision "serves as carte blanche for the United States to justify its restrictions on cross-border data flows."

The Trump administration also participated in a plurilateral negotiation under the aegis of the WTO's JSI, which began in 2017. After seven years of negotiations, in July 2024, some 91 nations agreed to a stabilized text, but that text did not include provisions on the free flow of data.[35] However, showing US influence, the stabilized text included provisions related to open public data in chapter 12. Building on US language, it states: "The Parties recognize that facilitating public access to and use of government data fosters economic and social development, competitiveness, and innovation."[36] To achieve that goal, governments "shall endeavour, to the extent practicable, to ensure that such data is: (a) made available in a machine-readable and open format; (b) searchable and retrievable; (c) updated, as applicable, in a timely manner; (d) accompanied by metadata that is, to the extent possible, based on commonly used formats that allow the user to understand and utilize the data; and (e) made generally available at no or reasonable cost to the user."[37] Moreover, "to the extent that a Party chooses to make government data digitally available for public access and use, it shall endeavour to avoid imposing conditions that unduly prevent or restrict the user of such data from (a) reproducing, redistributing, or republishing the data; (b) regrouping the data; or (c) using the data for commercial and non-commercial purposes, including in the process of producing a new product or service."[38] Hence, the language went beyond the Trump administration agreements, with aspirational language on metadata, updates and free or low-cost access to such data.

Meanwhile, the Japanese government sought to find ways to facilitate international agreement on cross-border data flows. In 2019, Shinzo Abe, then prime minister of Japan, stated that if the world wanted to achieve the benefits of the data-driven economy, members of the WTO should find a common approach to combining "data free flow with trust."[39] However, he never explained what these rules should look like and how nations might find an internationally accepted approach

30 *USMCA, supra* note 27, art 19.18(1).

31 Ibid, art 19.18(2).

32 Ibid, art 19.18(3). Equivalent language is contained within the *US-Japan Digital Trade Agreement, supra* note 29, art 20.

33 *USMCA, supra* note 27, art 32.2(1), online: <https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/32_Exceptions_and_General_Provisions.pdf>.

34 *US-Japan Digital Trade Agreement, supra* note 29, art 4, online: <https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf>.

35 See www.wto.org/english/tratop_e/ecom_e/joint_statement_e.html.

36 *JSI, supra* note 10, art 12.4, online: <https://clairk.digitalpolicyalert.org/documents/wto-agreement-on-electronic-commerce-july-2024-version/raw>.

37 Ibid, art 12.5.

38 See www.digital.go.jp/en/policies/dfft.

39 Ibid.

to such rules without a broad global discussion that showed that policy makers were responsive to public concerns about disinformation or manipulation (Aaronson 2023a; Arasasingham and Goodman 2023). Ever so gradually, various groups tried to bring the concept to life, focusing on how to reconcile the free flow of data with national security and privacy. The G7 committed to try to make DFFT a reality, noting that "trust should be built and realised through various legal and voluntary frameworks, guidelines, standards, technologies and other means that are transparent and protect data" (G7 2023, paragraph 6). In 2021 in the United Kingdom (G7 United Kingdom 2021), and in 2022 in Germany (G7 Germany 2022), policy makers worked out various road maps and action plans to achieving DFFT. Meanwhile, the OECD created an international community of experts to help operationalize the concept.[40] Although the United States participated in these efforts, US policy makers did not seem to view such statements as sufficient to address concerns about how DFFT could be made operational and, in so doing, address national security and privacy concerns.

In sum, the US position on the free flow of data changed slightly over time, reflecting both the concerns of other governments and its own policy gaps. Republican and Democratic administrations alike took the position that data should move freely among countries to facilitate business, innovation, education and democracy. In the more recent agreements, each government could decide whether to make data public, but they should be encouraged to make such government data available to all in a machine-readable format. Finally, policy makers argued that nations could rely on the WTO's exceptions if they needed to restrict cross-border flows, as long as such restrictions are necessary, limited and non-trade distorting. But US policy makers increasingly recognized that large troves of data could pose a national security risk. They began to not only clarify and expand the exception but also create specific domestic regulations on data that did not really address a key aspect of the problem: America's lack of a personal data protection law.

40 See www.oecd.org/en/about/programmes/data-free-flow-with-trust.html.

## The Biden Administration Rethinks the How and Where

As noted earlier, in 2021, President Biden issued an executive order[41] requiring the Secretary of Commerce to "evaluate data that poses a national security risk to Americans or the country as a whole."

But the Biden administration did not just bring a national security perspective to data governance; it also wanted to remake trade policy to benefit workers and rethink the tools governing digital markets. In 2021, then USTR Katherine Tai stated that digital trade must be "grounded in how it affects our people and our workers" (Office of the USTR 2021). The USTR would rethink its approach, focusing on whether the US digital trade agenda supports the broader national security interest and is flexible to meet future challenges. Tai went on to say that digital trade must be designed collaboratively with US allies "in a way that safeguards economic security for workers while protecting democracies against external threats" and balances "the right of governments to regulate in the public interest, with the need for rules" that guard against discriminatory behaviour (ibid.).

The Biden administration's rethink of digital trade was supported by groups such as the American Federation of Labor and Congress of Industrial Organizations (AFL-CIO) (America's umbrella trade union), Public Citizen,[42] the Center for Democracy & Technology, the American Civil Liberties Union[43] and the Rethink Trade program at the American Economic Liberties Project.[44] It was also supported by many members of Congress and the administration who felt strongly that the United States needed policy space and time to address the market power and human rights violations

41 *Protecting Americans, supra* note 2.

42 See www.citizen.org/article/digital-trade-sdgs/.

43 Letter from the American Civil Liberties Union, Centre for Democracy & Technology, Center for Digital Democracy, Data & Society Research Institute, Demand Progress Education Fund, Electronic Privacy Information Center, Fight for the Future et al. to President Biden (23 May 2023), online: <www.washingtonpost.com/documents/eea26d7a-08ef-4687-a4ba-c26e38ad7ffe.pdf?itid=lk_inline_manual_44>.

44 See www.economicliberties.us/rethink-trade/#.

caused by surveillance capitalism (Rangel and Wallach 2024). The AFL-CIO (2023) argued that while corporations could move, process and store data as they saw fit, workers were unprotected, and governments did not have to take "any meaningful action to protect individuals' personal data."

Meanwhile, the US Department of Commerce posited an alternative approach to governing cross-border data flows. It built on the 2004 Asia-Pacific Economic Cooperation (APEC) Privacy Framework — a set of nine principles providing guidance on implementation to assist the 21 members of APEC in developing consistent domestic approaches to personal information privacy protections. The Privacy Framework became a regional approach to promote accountable and responsible transfers of personal information between APEC economies; it was revised and updated in 2019 (APEC 2019). The United States partnered with Canada, Chinese Taipei, Japan, the Philippines, the Republic of Korea and Singapore to set up the Global CBPR System, a voluntary initiative that enabled firms to obtain data privacy certifications that helped demonstrate their compliance with internationally recognized data privacy standards. In so doing, the Biden administration could support the Japanese DFFT initiative by focusing on cooperation and compliance tools (US Department of Commerce 2022).[45] Participation in the CBPR is binding on the participants and can be enforced by national regulators of privacy. But participation is voluntary, and the certification is by the CBPR organization.[46] Hence, this approach was not so appealing in countries where personal data protection and strong enforcement is a priority. Nonetheless, the Biden administration hoped to extend this approach internationally and ensure it is interoperable with national privacy systems.[47] Secretary of Commerce Gina Raimondo described it as "the beginning of a new era of multilateral cooperation in promoting trusted global data flows....The new Forum will facilitate trade and international data flows...building on our shared data privacy values while recognizing the differences in our domestic approaches to protecting data privacy" (US Department of Commerce 2022).[48] However, that cooperation was limited to Asia. Moreover, it is unclear if the Trump administration will continue this approach.

Yet the United States did not abandon a shared international approach to data governance through trade agreement. The United States joined its G7 counterparts in announcing that G7 members must show progress toward advancing DFFT. Under this concept, personal data can be transferred across borders in a responsible, trustworthy manner while always adhering to high standards of data protection. However, no one knows how to create interoperable rules that yield DFFT. Nonetheless, the United States and its G7 counterparts kept trying to figure out what rules they should adopt, and how these rules must build and sustain trust among digital market actors (G7 2023). At the October 2024 meeting of the G7 Data Protection Authorities, the United States and its counterparts agreed to continue working on DFFT. "We highlight the need to rely on transfer mechanisms that ensure the protection of personal data when shared across borders, as this is an essential condition for data to be transferred safely and freely" (Office of the Privacy Commissioner of Canada 2024). The United States also continued to participate in efforts to ensure DFFT at the OECD, APEC, and other international meetings and organizations (ibid).[49] In 2023, the United States also worked with other APEC economies to develop and endorse new guidelines on facilitating access to open government data, "which will institutionalize inclusive approaches to commercial and government practices in the digital economy" (USTR 2024, 30).

Moreover, the United States continued to oppose direct and clear language on the free flow of data (and source code) in the JSI (Editorial Board 2023; Lawder 2023). Tai insisted that before it could further negotiate at the WTO, the United States needed to figure out how it could regulate privacy and big-tech business practices (Trachtenberg

45 See www.commerce.gov/global-cross-border-privacy-rules-declaration.

46 The participating organizations implement privacy policies and practices consistently with the CBPR program requirements. These privacy policies and practices should be evaluated by an APEC-recognized accountability agent for compliance with the CBPR program requirements. Once an organization has been certified for participation in the CBPR System, these privacy policies and practices will become binding as to that participant and will be enforceable by an appropriate authority, such as a regulator, to ensure compliance with the CBPR program requirements.

47 See www.commerce.gov/global-cross-border-privacy-rules-declaration.

48 Ibid.

49 See https://ustr.gov/issue-areas/services-investment/telecom-e-commerce; www.oecd.org/en/about/programmes/data-free-flow-with-trust.html. The author serves on an advisory body affiliated with this concept at the OECD.

2024). More recently, when the WTO issued a stabilized text for the JSI in July 2024, the United States explained its position was all about national security. After a broad text was made public, US Ambassador to the WTO Maria Pagan stated, "the current text falls short and more work is needed, including with respect to the essential security exception" (US Mission to International Organizations in Geneva 2024). She said the United States would work with other members to find shared solutions to conclude the JSI (ibid.).

Tai's approach toward the JSI was widely criticized by members of Congress and some in the business community. In March 2024, the chair of the House Committee on Oversight and Accountability launched an investigation over the alleged lack of consultations and the transparency of the USTR's communications with civil society (Trachtenberg 2024). Chairman James Comer (R-Ky.) noted it is Congress that must set the principles and objectives of US trade policy (Committee on Oversight and Government Reform 2024a, 2024b, 2024c). The USTR has not spoken publicly about the issue since the November 2024 presidential election.

Meanwhile, the Biden administration tried to convince the American public that the US government remains committed to rules encouraging the free flow of data and the sharing of open public data across borders (G7 2023; G7 Italia 2024; Government of Canada 2023).[50] For example, the US government sought public comment on these executive orders and held several meetings with academics, human rights groups, business representatives and others concerned about maintaining the free flow of data with limited exceptions. The author attended two such public meetings: one at the White House and another at the Center for Strategic & International Studies think tank, where senior White House officials from the National Economic Council and the National Security Council stressed that the United States remained committed to the free flow of data with limited exceptions.

Despite efforts at clarification, Biden policies on the free flow of data were confusing. The United States seemed to make domestic policy its main tool to address cross-border data. Moreover, the executive branch was not the only body acting on such restrictions. On April 24, 2024, President Biden signed PADFA into law.[51] The law prohibits "data brokers" from selling, licensing or transferring for consideration an American's "personally identifiable sensitive data" to certain "foreign adversary" countries — China, Iran, North Korea and Russia — *or* any entity "controlled" by those foreign adversary countries. PADFA applies to sensitive data sales to entities with 20 percent or more ownership by an individual or business domiciled or with a principal place of business in any of the foreign adversary countries. Further, the act applies to a broad set of "sensitive data," ranging from device geolocation data to certain information on "an individual's online activities." PADFA will be enforced by the FTC, which will be able to seek civil penalties for violations (Pozza et al. 2024).

## What Explains These Changes in the US Approach to Governing the Free Flow of Data?

No one reason can explain why the United States became more restrictive regarding cross-border data flows. Below, the author suggests several reasons.

**The public's and policy makers' understanding of data has changed over time, as data becomes ever more essential to the creation of AI tools.**

There is no AI without large pools of data that are often sourced globally. As the demand for data rises and the supply of data and data sets grows, the potential for hacking, theft, misinformation and other problems also increases (Aaronson 2020). However, developers, policy makers and users often do not know the provenance of the data they are relying on (how a data set was developed and where the data came from) and whether it can be trusted. People are increasingly aware that the data they provide and/or use may be data obtained without informed consent or appropriate enforcement. Finally, as various forms of data-driven technologies have come into wide

50 See https://g20.org/track/digital-economy-2/.

51 *Emergency supplemental appropriations, supra* note 3.

global use, policy makers have come to recognize that different types of data can pose risks when combined with personal data (Aaronson 2024b). For example, in 2019, the Pentagon asked military personnel to stop using at-home DNA kits for health and ancestry purposes, fearful that such data could be sold, hacked and crossed (Graff 2020). Moreover, new technologies such as virtual reality and wearables are creating new sources of data (virtual reality headsets and wearables can yield large volumes and new types of data in the form of eye blinks, sweat, blood pressure and so on). Such large troves of data could be hard to protect. Finally, policy makers acknowledge that America has become more restrictive on data flows due to the rising import of AI and competition with China on AI. According to Jake Sullivan, then President Biden's national security advisor, "The application of artificial intelligence will define the future, and our country must once again develop new capabilities, new tools, and… new doctrine, if we want to ensure that AI works for us, for our partners, for our interests, and for our values, and not against us….We know that China is building its own technological ecosystem with digital infrastructure that won't protect sensitive data, that can enable mass surveillance and censorship, that can spread misinformation, and that can make countries vulnerable to coercion….So, we have to compete to provide a more attractive path" (The White House 2024b).

**US policy makers decided that they must find ways to protect personal data, considering the failure to pass a national data protection law and mounting national security concerns about US adversaries stealing, collecting, and/or purchasing data and using that data.**

In the Trump administration trade agreements, "rather than carving out exceptions for data privacy, the United States has been establishing a 'national security bracket' to trade law. Sovereignty over national security policy, rather than the unmitigated free flow of data, is increasingly the name of the U.S. game….It is, therefore, not *individual* interests (or individual rights) but the *collective* interest in national security that the U.S. government understands to be at stake" (Irion, Kaminsky and Yakovleva 2023, italics in original). To reframe, instead of focusing on personal data as a human rights issue, which would require a data protection law, the US government is only focused on one aspect of data protection: when personal data could be collected, analyzed and manipulated in ways that threaten national security (ibid.). Moreover, law professors Anupam Chander and Paul M. Schwartz argue, "This growing executive branch power over personal data reflects a major shift in national security law: congressional delegations to the Executive have transformed individual choices about personal privacy into national security issues…. Just as there is a collective interest in national security, the law now recognizes a group interest in privacy" (Chander and Schwartz 2024, 1992).

**Congress has not set clear objectives and principles to govern trade policy, which meant the executive branch could make trade policy without public hearings, expert testimony and input from 435 diverse members of Congress**. It had not developed or passed legislation granting the executive branch the authority to negotiate trade policy since 2015 (Casey and Cimino-Isaacs 2024). Without such authority, it would be hard for the Biden administration or any administration to remake trade policy without broad input. But because Congress did not provide such guidance, the USTR could use executive agreements to approve the US-Japan Digital Trade Agreement or rely on the existing authority to update NAFTA. Moreover, the Biden administration could announce — at the WTO, rather than first consulting with Congress or America's allies — America's need for policy space on regulating technologies and cross-border data flows.

**Despite its strong cyber prowess, the United States has been unable to effectively protect data from theft, malware and manipulation.** Officials in the public and private sectors cannot consistently defend against cyber theft, manipulation, ransomware and hacking (Miller, Bazail-Eimil and Gramer 2024; Geller and Woodruff Swan 2020). As the sheer number of threats and adversaries mounts, and the scale and scope of data that organizations collect and hold continue to increase, defence is becoming more difficult (Government Accountability Office 2023). Dell (a US computer company) surveyed 1,500 information technology (IT) and IT security decision makers across the globe. Its most recent survey in 2023 found that 75 percent of organizations surveyed are worried their existing data protection measures are unable to cope with ransomware threats, and 69 percent reported they are not very confident they could reliably recover in the event of a destructive cyberattack. Eighty-one percent of organizations believe the rise in remote workers,

fuelled by the COVID-19 pandemic and still prevalent today, has increased their exposure to data loss from a cyberattack. This sentiment is up from 70 percent in 2022. Generative AI is having a significant impact on cybersecurity. Eighty-eight percent of organizations agree that generative AI is likely to generate large volumes of new data and increase the value of certain data types they need to consider when mapping out their future data protection strategies (Emsley 2024).

**The WTO has not provided guidance on when nations can restrict cross-border information, particularly in relation to protecting national security.** In fact, the United States sought guidance on the exceptions in a WTO trade dispute. Antigua challenged the US ban on internet gambling, and the WTO ruled that governments could restrict service exports to protect public morals — if those restrictions were necessary, proportionate and non-discriminatory.[52] But no member has challenged data flow restrictions for national security. Some scholars have suggested that these exceptions create uncertainty, and so policy makers should expand the exceptions to specifically include cybersecurity, privacy, online consumer protection and protecting public order to qualify as "legitimate public policy objectives" (Mitchell and Mishra 2021). Others have said that, in particular, policy makers must find ways to clarify the national security exceptions for data (Sun 2025).

# Conclusion

Is this the beginning of the end of the free flow of data? The author does not think so, but we are seeing a rebalancing. That rebalancing is not only happening in the United States.

US policy makers are increasingly willing to shift that balance in favour of protecting troves of data that could, when mixed with other data, pose a national security risk. Moreover, the United States did not abandon trade agreements as a tool to regulate such flows but created new approaches such as the IPEF or the CBPR. The country also turned to a domestic policy — excluding Congress and using executive orders.

This was not the first time the White House had limited some cross-border data flows; both the Reagan and Obama administrations adopted some limitations on cross-border data flows. Nonetheless, America's restrictions on data flows are consequential because some observers interpreted these policy strategies as major changes. These observers have a point. First, policy makers' reliance upon executive orders looks "protectionist." Moreover, US criticism of digital trade agreements and reluctance to sign on to them looks hypocritical. And since the United States did not notify its allies in advance or preview its revised stance with them, its actions likely undermined trust in America's commitment to open data flows. This decision is not likely to reinforce America's commitment to digital solidarity, which the US Department of State defined as "a willingness to work together on shared goals, to stand together, to help partners build capacity, and to provide mutual support."[53]

Several members of Congress and *The Wall Street Journal* argued in an editorial that the US actions empowered China, its key competitor in technological development (Cassidy 2023; Editorial Board 2023). These critics had a point: on November 21, 2024, the Chinese government pounced, announcing that China is committed to cross-border data flow cooperation; advocates for the principles of openness, inclusiveness, security, cooperation and non-discrimination; advances flow cooperation; and promotes efficient, smooth and secure cross-border data flow (State Council of the People's Republic of China 2024; chinadaily.com.cn 2024; *Global Times* 2024). But the Chinese government also signalled ambivalence about data. On December 2, 2024, the Chinese government warned that open-source information threatens national security by making sensitive data vulnerable to exploitation by foreign spies. Reporter Vanessa Cai wrote: "Sensitive data that is not properly declassified or assessed for risks can be publicly spread online and 'become an important source of open-source intelligence' for overseas spy agencies," quoting a statement

52 WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services,* Communication from Antigua and Barbuda, WTO Doc WT/DS285, Panel report circulated 10 November 2004 (adopted 20 April 2005), Appellate Body report circulated 7 April 2005 (adopted 20 April 2005), online: <www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm>.

53 See www.state.gov/building-digital-solidarity-the-united-states-international-cyberspace-and-digital-policy-strategy/.

by the Ministry of State Security in an article posted on its official WeChat account (Cai 2024).

While the United States has so far limited these executive orders to adversaries, some proclaimed that these rules were a form of data sovereignty (Burman 2023; Chaudhuri and Kang 2024). But the United States is not saying it must be sovereign over the personal data of Americans. Moreover, the US policy of balancing privacy, national security and cross-border data flows is not unique. According to scholars at the University of Lucerne, which houses a large data set of trade agreements, most such agreements contain exceptions and carve-outs. These exceptions and carve-outs provide policy space to achieve the desired national balance of open data flows and national security and/or privacy (Burri, Vásquez Callo-Müller and Kugler 2024). Unfortunately, there have been few trade disputes related to these exceptions, so policy makers do not know how and when they can use these exceptions without being challenged by a trade partner(s).

National security data restrictions could prove difficult to dismantle and may spread to other data types and uses. Advocates of the data-driven economy should pay close attention because these restrictions occur at a time when more firms and governments are hoarding data (Leetaru 2019; Heikkilä 2024; Braue 2021), and some analysts argue we are running out of data for various types of AI (Jones 2024; *The Economist* 2024; Roose 2024). In fact, in response to Trump tariff threats in April 2025, French Economy and Finance Minister Eric Lombard suggested that France could "strengthen certain administrative requirements or regulate the use of data" (Haeck 2025).

Moreover, US restrictions could hurt the US AI lead. AI developers often need large pools of data to ensure that they are developing the most accurate, complete and representative data sets. These restrictions could also reduce the potential of AI as a public good. If data can flow freely across borders, it can be used by a wide range of market actors and society and generate new, ever more valuable applications that combine data in new ways. If data becomes inaccessible or siloed, it is a market failure because data is more valuable when individuals who can see its potential can aggregate and analyze it (Koutroumpis, Leiponen and Thomas 2020; Aaronson 2023b).

The current Trump administration has not clarified its position on the free flow of data or openness. It has, however, issued various executive orders on the use of data. For example, it issued an executive order designed to encourage agencies to share data and prevent information silos (The White House 2025a). Some observers worried that such information sharing could violate the privacy rights of Americans, allowing agencies to use data collected for one purpose to be used for another — a potential crime (Alms 2025; Hengesbaugh and Feiler 2025). In May 2025, it issued another executive order that stated, "this order restores the scientific integrity policies of my first Administration and ensures that agencies practice data transparency, acknowledge relevant scientific uncertainties, are transparent about the assumptions and likelihood of scenarios used, approach scientific findings objectively, and communicate scientific data accurately. Agency use of Gold Standard Science, as set forth in this order, will spur innovation, translate discovery to success, and ensure continued American strength and global leadership in technology" (The White House 2025b). Despite these pretty words, the current Trump administration has cut funding for economics and statistical advisory committees, and stopped sharing information about climate change, diversity statistics and other policies (Jones 2025; Laird, Woelfel and Anex-Ries). America's role in encouraging the free flow of data within the United States and around the world could be on the decline.

Additionally, restrictions on open data and the free flow of data could undermine American leadership in science. Scientific and technological development is global, and researchers in the United States and China often collaborate and compete to create breakthroughs (Delaney 2024). The second Trump administration has made drastic cuts to National Institutes of Health and National Science Foundation funding (Wadman 2025; Garisto and *Nature Magazine* 2025). Such dramatic policy changes create uncertainty, which can undermine the trust that is essential to the data-driven economy and scientific progress.

Finally, selective restrictions on data flows are policy "whack-a-mole." The United States should get its own house in order and develop comprehensive data protection rules. In 2024, it looked like Congress was making progress. In April, the chair of the House Committee on Energy and Commerce,

Cathy McMorris Rodgers (R-WA), and Senate Commerce Chair Maria Cantwell (D-WA) introduced the American Privacy Rights Act. The act would prohibit the use of certain types of personal data to discriminate against consumers and provide them with the right to opt out of the use of algorithms for consequential decisions. The FTC, state attorneys general and consumers could enforce against violations of the act.[54] But as of this writing, the bill has not moved forward in either body.

Given the import of this issue, one must wonder why it is so hard to pass data protection laws in the United States. One explanation could be business opposition and ambivalence: many of the biggest firms claim to want data protection laws, but they rarely support the major bills. Meanwhile, gridlock and party differences provide another possible explanation. According to the Congressional Research Service, policy makers must consider if the law is outcome-based or prescriptive, how protected information is defined, which agency will enforce the law and who should be held liable for violations. Many states already have data protection laws; in turn, federal pre-emption will be an issue. Finally, from a First Amendment perspective, Supreme Court jurisprudence suggests that while some privacy, cybersecurity or data security regulations are permissible, any federal law that restricts protected speech, particularly if it targets specific speakers or content, may be subject to more stringent evaluation by a reviewing court (Mulligan and Linebaugh 2022, 2). Thus, it is not easy to draft and come to a consensus on such laws. But even if the United States did finalize such a law, it would not effectively ensure the free flow of data (Chander and Schwartz 2024).

The OECD recently issued a report that showed many nations are restricting cross-border data flows for a wide range of reasons, including to protect privacy and national security. It argued that these restrictions have a significant cost to the economy (López González, Del Giovane and Ferencz 2025). Policy makers generally rely on self-judging trade agreement exceptions to justify these restrictions (ibid., 21–24).

The free flow of data is generally a public good, and most data should flow freely. But many types of data can have intelligence value, especially when mixed with other data sets. Foreign governments and non-state actors can purchase or hack such data and misuse it in ways that make individuals and the nation vulnerable (Ryan and Christl 2023). So, instead of putting forward whack-a-mole policy, US officials must find interoperable tools and strategies, working with US allies to clarify how and when policy makers can restrict access to data flowing across borders (Faveri et al. 2025; APEC Committee on Trade and Investment 2023).

In a 2013 article, Kenneth Cukier and Viktor Mayer-Schoenberger (2013) warned that we would need new ways of thinking about data and datafication, as data changes how we see the world. The world would benefit from a more comprehensive analysis of the costs and benefits of openness and the free flow of data. It seems likely that openness and the free flow of data benefit transparency, science, accountability and good governance. However, the sheer volume of data and disinformation may also make it easier to undermine democracy. Finally, in the age of generative AI, corporations seem to be capturing much of the value of data while individuals and governments are losing control.

54 US, Bill HR 8818, *American Privacy Rights Act of 2024*, 118th Cong, 2024 (not yet enacted), online: <www.congress.gov/bill/118th-congress/house-bill/8818>.

## Works Cited


Aaronson, Susan. 2016. *The Digital Trade Imbalance and Its Implications for Internet Governance*. Global Commission on Internet Governance Paper No. 25. Waterloo, ON: CIGI. www.cigionline.org/publications/digital-trade-imbalance-and-its-implications-internet-governance/.

———. 2020. *Data Is Dangerous: Comparing the Risks That the United States, Canada and Germany See in Data Troves*. CIGI Paper No. 241. Waterloo, ON: CIGI. www.cigionline.org/publications/data-dangerous-comparing-risks-united-states-canada-and-germany-see-data-troves.

———. 2023a. "US Reversal on Digital Trade Undermines America's Credibility." Opinion, Centre for International Governance Innovation, December 14. www.cigionline.org/articles/us-reversal-on-digital-trade-undermines-americas-credibility/.

———. 2023b. *Could a Global "Wicked Problems Agency" Incentivize Data Sharing?* CIGI Paper No. 273. Waterloo, ON: CIGI. www.cigionline.org/publications/could-a-global-wicked-problems-agency-incentivize-data-sharing/.

———. 2024a. *Data Disquiet: Concerns about the Governance of Data for Generative AI*. CIGI Paper No. 290. Waterloo, ON: CIGI. www.cigionline.org/publications/data-disquiet-concerns-about-the-governance-of-data-for-generative-ai/.

———. 2024b. "Data Governance Is Not Ready for AI." The Role of Governance in Unleashing the Value of Data Essay Series, Centre for International Governance Innovation, November 12. www.cigionline.org/the-role-of-governance-in-unleashing-the-value-of-data/.

Aaronson, Susan Ariel and Thomas Struett. 2020. *Data Is Divisive: A History of Public Communications on E-commerce, 1998–2020*. CIGI Paper No. 247. Waterloo, ON: CIGI. www.cigionline.org/publications/data-divisive-history-public-communications-e-commerce-1998-2020/.

AFL-CIO. 2023. "A Worker-Centered Digital Trade Agenda." February 7. https://aflcio.org/worker-centered-digital-agenda.

Alms, Natalie. 2025. "Trump pens executive order pushing agencies to share data." Nextgov/FCW, March 21. www.nextgov.com/digital-government/2025/03/trump-pens-executive-order-pushing-agencies-share-data/403962/.

Alschner, Wolfgang. 2023. "E-commerce or digital trade? Why the difference should matter to trade lawyers." In *Research Handbook on Digital Trade*, edited by David Collins and Michael Geist, 54–72. Cheltenham, UK: Edward Elgar. www.e-elgar.com/shop/usd/research-handbook-on-digital-trade-9781800884946.html.

APEC. 2019. "APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines." November. https://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf.

APEC Committee on Trade and Investment. 2023. *Economic Impact of Adopting Digital Trade Rules: Evidence from APEC Member Economies*. March. Singapore: APEC Secretariat. www.apec.org/publications/2023/04/economic-impact-of-adopting-digital-trade-rules-evidence-from-apec-member-economies.

Arasasingham, Aidan and Matthew P. Goodman. 2023. "Operationalizing Data Free Flow with Trust (DFFT)." Center for Strategic & International Studies, April 13. www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft.

Baldwin, Richard. 2022. "The peak globalisation myth: Part 4 – Services trade did not peak." VoxEU, September 3. https://cepr.org/voxeu/columns/peak-globalisation-myth-part-4-services-trade-did-not-peak/.

Bella, Kimberly and Supheakmungkol Sarin. 2023. "Free-flowing data is good for people and the global economy." World Economic Forum, January 16. www.weforum.org/stories/2023/01/enabling-free-flows-of-data-a-user-centric-approach/.

Berliner, Daniel. 2014. "The Political Origins of Transparency." *Journal of Politics* 76 (2): 479–91. https://doi.org/10.1017/s0022381613001412.

Braue, David. 2021. "Why Companies Are Hoarding Your Personal Data." *Cybercrime Magazine*, April 13. https://cybersecurityventures.com/why-companies-are-hoarding-your-personal-data/.

Broadbent, Meredith. 2023. "USTR Upends U.S. Negotiating Position on Cross-Border Data Flows." Center for Strategic & International Studies, December 12. www.csis.org/analysis/ustr-upends-us-negotiating-position-cross-border-data-flows.

Brown, Evan, Caitlin Chin-Rothmann and Julia Brock. 2024. "Exploring the White House's Executive Order to Limit Data Transfers to Foreign Adversaries." Center for Strategic & International Studies, February 29. www.csis.org/analysis/exploring-white-houses-executive-order-limit-data-transfers-foreign-adversaries.

Burman, Anirudh. 2023. "Understanding India's New Data Protection Law." Carnegie Endowment for International Peace, October 3. https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en.

Burri, Mira, María Vásquez Callo-Müller and Kholofelo Kugler. 2024. "The Evolution of Digital Trade Law: Insights from TAPED." *World Trade Review* 23 (2): 190–207. https://doi.org/10.1017/S1474745623000472.

Cai, Vanessa. 2024. "China's intelligence ministry warns of security risks from open-source information." *South China Morning Post*, December 2. www.scmp.com/news/china/politics/article/3288946/chinas-spy-ministry-warns-national-security-risks-open-source-information.

Casey, Christopher A. and Cathleen D. Cimino-Isaacs. 2024. "Trade Promotion Authority (TPA)." Congressional Research Service, February 20. www.congress.gov/crs-product/IF10038.

Cassidy, Bill. 2023. "Cassidy, Wyden, Crapo Call on White House to Reverse Course on Digital Trade and Stand Up to China, Support American Workers and Human Rights." Press release, November 30. www.cassidy.senate.gov/newsroom/press-releases/cassidy-wyden-crapo-call-on-white-house-to-reverse-course-on-digital-trade-and-stand-up-to-china-support-american-workers-and-human-rights/.

Chander, Anupam and Paul Schwartz. 2024. "The President's Authority over Cross-Border Data Flows." *University of Pennsylvania Law Review* 172 (7): 1989–2052. https://scholarship.law.georgetown.edu/facpub/2625.

Chaudhuri, Rudra and Arjun Kang Joseph. 2024. "Living in a fragmented world: India's data way." *India Review* 23 (2): 154–76. https://doi.org/10.1080/14736489.2024.2324638.

chinadaily.com.cn. "China has potential to take the lead in global digital trade, says former commerce vice-minister." November 18. www.chinadaily.com.cn/a/202411/18/WS673b02a4a310f1265a1ce1cf.html.

Ciuriak, Dan and Vlada Rodionova. 2021. "Trading Artificial Intelligence: Economic Interests, Societal Choices, and Multilateral Rules." In *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration*, edited by Shin-yi Peng, Ching-Fu Lin and Thomas Streinz, 70–94. Cambridge, UK: Cambridge University Press.

Committee on Oversight and Government Reform. 2024a. "Comer Outlines USTR's Inadequate Cooperation with Probe into Abandoned Digital Trade Commitments, Renews Transcribed Interview Request." Press release, July 11. https://oversight.house.gov/release/comer-outlines-ustrs-inadequate-cooperation-with-probe-into-abandoned-digital-trade-commitments-renews-transcribed-interview-request/.

———. 2024b. "Comer Requests NGOs to Preserve Docs Related to USTR Decision to Abandon U.S. Digital Trade Commitments." Press release, March 27. https://oversight.house.gov/release/comer-requests-ngos-to-preserve-docs-related-to-ustr-decision-to-abandon-u-s-digital-trade-commitments/.

———. 2024c. "Comer Probes USTR's Lack of Transparency, Secretive Communications." Press release, March 4. https://oversight.house.gov/release/comer-probes-ustrs-lack-of-transparency-secretive-communications.

Corey, Nigel. 2024. "If China Is Weaponizing Access to U.S. Data, We Need to See the Evidence." Information Technology & Innovation Foundation, April 5. https://itif.org/publications/2024/04/05/if-china-is-weaponizing-access-to-us-data-we-need-to-see-the-evidence/.

Cukier, Kenneth and Viktor Mayer-Schoenberger. 2013. "The Rise of Big Data: How It's Changing the Way We Think About the World." *Foreign Affairs* 92 (3): 28–40. www.jstor.org/stable/23526834.

Davis+Gilbert. 2023. "U.S. Data Broker Legislation Expands to Include Texas and Oregon." November 27. www.dglaw.com/u-s-data-broker-legislation-expands-to-include-texas-and-oregon/.

Dearden, Nick. 2016. "TTIP was defeated by activists — Trump just exploited public anger over it." *The Guardian*, November 14. www.theguardian.com/commentisfree/2016/nov/14/ttip-defeated-activists-donald-trump.

Delaney, Robert. 2024. "US must engage China's 'wickedly competitive' hi-tech firms: trade group leader." *South China Morning Post*, December 11. www.scmp.com/news/china/science/article/3290230/us-must-engage-chinas-wickedly-competitive-hi-tech-firms-trade-group-leader.

Drake, William J. 1993. "Territoriality and Intangibility: Transborder Data Flows and National Sovereignty." In *Beyond National Sovereignty: International Communications in the 1990s*, edited by Kaarle Nordenstreng and Herbert I. Schiller, 259–313. Norwood, NJ: Ablex.

Drake, William J. and Kalypso Nicolaïdis. 2000. "Global Electronic Commerce and GATS: The 'Millennium Round' and Beyond." In *GATS 2000: New Directions in Services Trade Liberalization*, edited by Pierre Sauve and Robert M. Stern, 399–437. Washington, DC: Brookings Institution.

Dupont, Dan. 2023. "U.S. to end support for WTO e-commerce proposals, wants 'policy space' for digital trade rethink." World Trade Online, October 24. https://insidetrade.com/daily-news/us-end-support-wto-e-commerce-proposals-wants-policy-space-digital-trade-rethink.

Editorial Board. 2023. "President Biden's Trade Gift to China." *The Wall Street Journal*, November 14. www.wsj.com/articles/indo-pacific-economic-framework-digital-trade-biden-administration-42be6640.

Emsley, Rob. 2024. "Charting a Path to Cyber Resilient Data Protection." *Dell Blog*, January 9. www.dell.com/en-us/blog/charting-a-path-to-cyber-resilient-data-protection/.

Faveri, Benjamin, Craig Shank, Richard Whitt and Philip Dawson. 2025. "The Need for and Pathways to AI Regulatory and Technical Interoperability." Tech Policy Press, April 16. www.techpolicy.press/the-need-for-and-pathways-to-ai-regulatory-and-technical-interoperability/.

Florini, Ann. 1998. "The End of Secrecy." *Foreign Policy* 111: 50–63. https://doi.org/10.2307/1149378.

Funk, Allie and Jennifer Brody. 2023. "Reversal of US Trade Policy Threatens the Free and Open Internet." Tech Policy Press, November 14. www.techpolicy.press/reversal-of-us-trade-policy-threatens-the-free-and-open-internet/.

———. 2024. "The Human Rights Costs of Data Localization Around the World." Tech Policy Press, March 26. www.techpolicy.press/the-human-rights-costs-of-data-localization-around-the-world/.

G7. 2023. "Ministerial Declaration: The G7 Digital and Tech Ministers' Meeting." G7 2023 Hiroshima Summit, April 30. https://g7g20-documents.org/database/document/2023-g7-japan-ministerial-meetings-ict-ministers-ministers-language-ministerial-declaration-the-g7-digital-and-tech-ministers-meeting.

G7 Germany. 2022. "G7 Digital Ministers' Track – Annex 1: G7 Action Plan for Promoting Data Free Flow with Trust." www.bmv.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-final-declaration-annex-1.pdf.

G7 Italia. 2024. "G7 Industry, Technology and Digital Ministerial Meeting." Verona and Trento, Italy, March 14–15. www.g7.utoronto.ca/ict/2024-declaration.html.

G7 United Kingdom. 2021. "G7 Digital and Technology Track – Annex 2: G7 Roadmap for Cooperation on Data Free Flow with Trust." https://assets.publishing.service.gov.uk/media/609cf5e18fa8f56a3c162a43/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf.

Garisto, Dan and *Nature Magazine*. 2025. "Trump Administration's Science Cuts Come for NSF Funding." *Scientific American*, April 18. www.scientificamerican.com/article/trump-administrations-science-cuts-come-for-nsf-funding/.

Geller, Eric and Betsy Woodruff Swan. 2020. "DOJ says Chinese hackers targeted coronavirus vaccine research." *Politico*, July 21. www.politico.com/news/2020/07/21/doj-chinese-hackers-coronavirus-research-375855.

*Global Times*. 2024. "Global Cross-Border Data Flow Cooperation Initiative showcases China's firm resolve to improve digital governance: FM spokesperson." November 20. www.globaltimes.cn/page/202411/1323453.shtml.

Government Accountability Office. 2023. *Global Cybercrime: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime*. GAO-23-104768. March 1. www.gao.gov/products/gao-23-104768.

———. 2024. *Foreign Disinformation: Defining and Detecting Threats*. GAO-24-107600. September 26. www.gao.gov/products/gao-24-107600.

Government of Canada. 2023. "G7 Hiroshima Leaders' Communiqué." May 20. www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2023-05-20-hiroshima-leaders-communique-dirigeants.aspx?lang=eng.

Haeck, Pieter. 2025. "France suggests targeting Big Tech's data use in response to US tariffs." *Politico*, April 6. www.politico.eu/article/france-suggest-to-regulate-data-in-response-to-trump-tariffs/.

Heikkilä, Melissa. 2024. "AI companies are finally being forced to cough up for training data." *MIT Technology Review*, July 2. www.technologyreview. com/2024/07/02/1094508/ai-companies-are-finally-being-forced-to-cough-up-for-training-data/.

Hengesbaugh, Brian and Lukas Feiler. 2025. "How could Trump administration actions affect the EU-US Data Privacy Framework?" International Association of Privacy Professionals, February 26. https://iapp.org/news/a/how-could-trump-administration-actions-affect-the-eu-u-s-data-privacy-framework-.

Hsu, Jeremy. 2018. "The Strava Heat Map and the End of Secrets." *Wired*, January 29. www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

Irion, Kristina, Margot E. Kaminski and Svetlana Yakovleva. 2023. "Privacy Peg, Trade Hole: Why We (Still) Shouldn't Put Data Privacy in Trade Law." *University of Chicago Law Review*, March 27. https://lawreview.uchicago.edu/online-archive/privacy-peg-trade-hole-why-we-still-shouldnt-put-data-privacy-trade-law.

Jones, Claire. 2025. "US economic data at risk from Elon Musk's Doge cuts." *Financial Times*, March 27. www.ft.com/content/57ef7cef-3391-4282-bdb7-a4a0186370cd.

Jones, Nicola. 2024. "The AI revolution is running out of data. What can researchers do?" *Nature*, December 11. www.nature.com/articles/d41586-024-03990-2.

Koutroumpis, Pantelis, Aija Leiponen and Llewellyn D. W. Thomas. 2020. "Markets for data." *Industrial and Corporate Change* 29 (3): 645–60. https://doi.org/10.1093/icc/dtaa002.

Laird, Elizabeth, Kristin Woelfel and Quinn Anex-Ries. 2025. "CDT and The Leadership Conference Release New Analysis of DOGE, Government Data, and Privacy Trends." Center for Democracy & Technology, March 19. https://cdt.org/insights/cdt-and-the-leadership-conference-release-new-analysis-of-doge-government-data-and-privacy-trends/.

Lanoszka, Alexander. 2019. "Disinformation in international politics." *European Journal of International Security* 4 (2): 227–48. https://doi.org/10.1017/eis.2019.6.

Lawder, David. 2023. "US drops digital trade demands at WTO to allow room for stronger tech regulation." Reuters, October 25. www.reuters.com/world/us/us-drops-digital-trade-demands-wto-allow-room-stronger-tech-regulation-2023-10-25/.

Leetaru, Kalev. 2019. "AI & Big Data's Hoarding Mentality Creates A New Era Of Cyber Risks." *Forbes*, August 29. www.forbes.com/sites/kalevleetaru/2019/08/29/ai--big-datas-hoarding-mentality-creates-a-new-era-of-cyber-risks/.

Lester, Simon. 2023. "The U.S. Changes Its Mind in the WTO E-Commerce Negotiations." *International Economic Law and Policy Blog*, October 30. https://ielp.worldtradelaw. net/2023/10/the-us-changes-its-mind-in-the-wto-e-commerce-negotiations.html.

López González, Javier, Chiara Del Giovane and Janos Ferencz. 2025. "A Preliminary Mapping of Measures Affecting the Cross-Border Flow of Non-Personal Data." OECD Trade Policy Papers No. 295. www.oecd.org/en/publications/a-preliminary-mapping-of-measures-affecting-the-cross-border-flow-of-non-personal-data_0825c57c-en.html.

Lucas, Edward. 2019. "The Spycraft Revolution." *Foreign Policy*, April 27. https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/.

MacGillis, Alec. 2025. "Trump's War on Measurement Means Losing Data on Drug Use, Maternal Mortality, Climate Change and More." *ProPublica*, April 18. www.propublica.org/article/trump-doge-data-collection-hhs-epa-cdc-maternal-mortality.

Mendel, Toby. n.d. "Freedom of Information as an Internationally Protected Human Right." Article 19. www.article19.org/data/files/pdfs/publications/foi-as-an-international-right.pdf.

Miller, Maggie, Eric Bazail-Eimil and Robbie Gramer. 2024. "We need to talk about Salt Typhoon." *Politico*, December 12. www.politico.com/newsletters/national-security-daily/2024/12/12/we-need-to-talk-about-salt-typhoon-00183727.

Mitchell, Andrew D. and Neha Mishra. 2021. "WTO Law and Cross-Border Data Flows: An Unfinished Agenda." In *Big Data and Global Trade Law*, edited by Mira Burri, 83–112. www.cambridge.org/core/books/big-data-and-global-trade-law/wto-law-and-crossborder-data-flows/FC0CF4A171B57CB6BF4F7CE96C5F1D45.

Monteiro, José-Antonio and Robert Teh. 2017. "Provisions on Electronic Commerce in Regional Trade Agreements." WTO Working Paper ERSD-2017-11. July. WTO Economic Research and Statistics Division. www.wto.org/english/res_e/reser_e/ersd201711_e.htm.

Mulligan, Stephen P. and Chris D. Linebaugh. 2022. "Data Protection and Privacy Law: An Introduction." Congressional Research Service, February 12 (updated October 12). www.congress.gov/crs-product/IF11207#:~:text.

Natanson, Hannah. 2025. "The first rule in Trump's Washington: Don't write anything down." *The Washington Post*, June 29. www.washingtonpost.com/politics/2025/06/29/first-rule-trumps-washington-dont-write-anything-down/.

National Intelligence Council. 2021. *Global Trends 2040: A More Contested World*. March. Washington, DC: Office of the Director of National Intelligence. www.dni.gov/files/images/globalTrends/GT2040/GlobalTrends_2040_for_web1.pdf.

OECD. 2015. *Data-Driven Innovation: Big Data for Growth and Well-being*. Paris, France: OECD. http://dx.doi.org/10.1787/9789264229358-en.

———. 2022. *Going Digital to Advance Data Governance for Growth and Well-Being*. Paris, France: OECD. www.oecd.org/en/publications/going-digital-to-advance-data-governance-for-growth-and-well-being_e3d783b0-en.html.

OECD and World Trade Organization. 2025. *Economic Implications of Data Regulation: Balancing Openness and Trust*. Paris, France: OECD. https://doi.org/10.1787/aa285504-en.

Office of the Privacy Commissioner of Canada. 2024. "G7 Data Protection and Privacy Authorities' Communiqué." Roundtable of G7 Data Protection and Privacy Authorities, October 11. www.priv.gc.ca/en/opc-news/news-and-announcements/2024/communique-g7_241011/.

Office of the USTR. 2021. "Remarks of Ambassador Katherine Tai on Digital Trade at the Georgetown University Law Center Virtual Conference." November. https://ustr.gov/about-us/policy-offices/press-office/speeches-and-remarks/2021/november/remarks-ambassador-katherine-tai-digital-trade-georgetown-university-law-center-virtual-conference.

Posetti, Julie and Alice Matthews. 2018. "A short guide to the history of 'fake news' and disinformation." International Center for Journalists, July. www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf.

Pozza, Duane C., Nazak Nikakhtar, Kathleen E. Scott and Stephanie Rigizadeh. 2024. "New Federal Data Broker Law Will Restrict Certain Foreign Data Sales Effective June 23." Wiley, May 7. www.wiley.law/alert-New-Federal-Data-Broker-Law-Will-Restrict-Certain-Foreign-Data-Sales-Effective-June-23.

Rangel, Daniel and Lori Wallach. 2024. "Trade Pacts Should Not Have Special Secrecy Guarantees for Source Code & Algorithms." Trade Policy Press, February 12. www.techpolicy.press/trade-pacts-should-not-have-special-secrecy-guarantees-for-source-code-algorithms/.

Rashid, Fahmida Y. 2014. "Surveillance is the Business Model of the Internet: Bruce Schneier." SecurityWeek, April 9. www.schneier.com/news/archives/2014/04/surveillance_is_the.html.

Reichman, Jerome H. and Keith E. Maskus. 2004. "The Globalization of Private Knowledge Goods and the Privatization of Global Public Goods." *Journal of International Economic Law 7* (2): 279–320. https://doi.org/10.1093/jiel/7.2.279.

Reuters. 2024. "Eighty nations strike deal over e-commerce, but lack US backing." July 26. www.reuters.com/markets/eighty-nations-strike-deal-over-e-commerce-lack-us-backing-2024-07-26/.

Roose, Kevin. 2024. "The Data That Powers AI Is Disappearing Fast." *The New York Times*, July 19. www.nytimes.com/2024/07/19/technology/ai-data-restrictions.html.

Rule, Sheila. 1989. "Reagan Gets A Red Carpet From British." *The New York Times*, June 14. www.nytimes.com/1989/06/14/world/reagan-gets-a-red-carpet-from-british.html.

Ryan, Johnny and Wolfie Christl. 2023. *America's hidden security crisis*. November 14. Dublin, Ireland: Irish Council for Civil Liberties. www.iccl.ie/digital-data/americas-hidden-security-crisis/.

Southerton, Clare. 2020. "Datafication." In *Encyclopedia of Big Data*, edited by Laurie A. Schintler and Connie L. McNeely, 358–61. Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-32001-4_332-1.

State Council of the People's Republic of China. 2024. "China ready to deepen int'l cooperation on cross-border data flow: spokesperson." November 21. https://english.www.gov.cn/news/202411/21/content_WS673e9f5dc6d0868f4e8ed483.html.

Sun, Qi. 2025. "The Study on Exception Clauses of Cross-Border Data Flows in International Trade Agreements." *Journal of Theory and Practice in Humanities and Social Sciences* 2 (2): 1–18. https://woodyinternational.com/index.php/jtphss/article/view/177.

*The Economist*. 2024. "AI firms will soon exhaust most of the internet's data." July 27. www.economist.com/schools-brief/2024/07/23/ai-firms-will-soon-exhaust-most-of-the-internets-data.

The White House. 2013. "Executive Order – Making Open and Machine Readable the New Default for Government Information." Press release, May 9. https://obamawhitehouse.archives.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government-.

———. 2024a. "What Drives the U.S. Services Trade Surplus? Growth in Digitally-Enabled Services Exports." Council of Economic Advisers, Written Materials, June 10. https://bidenwhitehouse.archives.gov/cea/written-materials/2024/06/10/what-drives-the-u-s-services-trade-surplus-growth-in-digitally-enabled-services-exports/.

———. 2024b. "Remarks by APNSA Jake Sullivan on AI and National Security." Speeches and Remarks, October 24. https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2024/10/24/remarks-by-apnsa-jake-sullivan-on-ai-and-national-security/.

———. 2025a. "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos." Executive Order, March 20. www.whitehouse.gov/presidential-actions/2025/03/stopping-waste-fraud-and-abuse-by-eliminating-information-silos/.

———. 2025b. "Restoring Gold Standard Science." Executive Order, May 23. www.whitehouse. gov/presidential- actions/2025/05/restoring-gold-standard-science/.

Trachtenberg, Danielle M. 2024. "Digital Trade and Data Policy: Key Issues Facing Congress." Congressional Research Service, July 30. www.congress.gov/crs-product/IF12347.

United Nations Conference on Trade and Development. 2021. *Digital Economy Report 2021 – Cross-border data flows and development: For whom the data flow*. New York, NY: United Nations. https://unctad.org/page/digital-economy-report-2021.

———. 2023. *G20 Members' Regulations of Cross-Border Data Flows*. UNCTAD/DTL/ECDE/2023/1. Geneva, Switzerland: United Nations. https://unctad.org/publication/g20-members-regulations-cross-border-data-flows.

US Department of Commerce. 2022. "Statement by Commerce Secretary Raimondo on Establishment of the Global Cross-Border Privacy Rules (CBPR) Forum." Press release, April 21. www.commerce.gov/news/press-releases/2022/04/statement-commerce-secretary-raimondo-establishment-global-cross-border.

US Department of Justice. 2024. "Justice Department Issues Final Rule Addressing Threat Posed by Foreign Adversaries' Access to Americans' Sensitive Personal Data." Press release, December 27. www.justice.gov/opa/pr/justice-department-issues-final-rule-addressing-threat-posed-foreign-adversaries-access.

US Mission to International Organizations in Geneva. 2024. "Statement by Ambassador María L. Pagán on the WTO E-Commerce Joint Statement Initiative." July 26. https://geneva.usmission.gov/2024/07/26/statement-by-ambassador-maria-l-pagan-on-the-wto-e-commerce-joint-statement-initiative/.

USTR. 2015. "Fact Sheet: Transparency and the Obama Trade Agenda." January. https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2015/january/fact-sheet-transparency-and-obama.

———. 2016a. "The Digital 2 Dozen." https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2016/digital-2-dozen.

———. 2016b. *2016 Trade Policy Agenda and 2015 Annual Report of the President of the United States on the Trade Agreements Program.* Washington, DC: USTR. https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2016/2016-trade-policy-agenda-and-2015-Annual-Report.

———. 2017a. "The United States Officially Withdraws from the Trans-Pacific Partnershp." Press release, January. https://ustr.gov/about-us/policy-offices/press-office/press-releases/2017/january/US-Withdraws-From-TPP.

———. 2017b. "Key Barriers to Digital Trade." March. https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade.

———. 2019. *2019 Trade Policy Agenda and 2018 Annual Report of the President of the United States on the Trade Agreements Program.* Washington, DC: USTR. https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2019/2019-trade-policy-agenda-and-2018.

———. 2023. "USTR Statement on WTO E-Commerce Negotiations." Press release, October 24. https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/october/ustr-statement-wto-e-commerce-negotiations.

———. 2024. *2024 Trade Policy Agenda and 2023 Annual Report of the President of the United States on the Trade Agreements Program.* March. Washington, DC: USTR. https://ustr.gov/sites/default/files/The%20Presidents%202024%20Trade%20Policy%20Agenda%20and%202023%20Annual%20Report.pdf.

Van Dijck, José. 2020. "Open Societies and the Technical-Digital Perspective." In *The Open Society and Its Future,* edited by Mark Bovens and Marcus Düwell, 12–16. Think Paper Series No. 1. Utrecht, the Netherlands: Institutions for Open Societies, Utrecht University. www.uu.nl/en/research/institutions-for-open-societies/ios-think-paper-series.

van Ham, Peter. 2016. "TTIP is dead, long live transatlantic trade." Clingendael, August 30. www.clingendael.org/publication/ttip-dead-long-live-transatlantic-trade.

Wadman, Meredith. 2025. "Trump proposes massive NIH budget cut and reorganization." *Science,* April 17. www.science.org/content/article/trump-proposes-massive-nih-budget-cut-and-reorganization.

WTO. 2024. *Trading with intelligence: How AI shapes and is shaped by international trade.* Geneva, Switzerland: WTO. www.wto.org/english/res_e/publications_e/trading_with_intelligence_e.htm.

Wugmeister, Miriam H., Joseph Charles Folio III and Carson Martinez. 2024. "Prohibitions on Data Broker Sales to Foreign Adversaries Just Expanded." Morrison Foerster, May 6. www.mofo.com/resources/insights/240506-prohibitions-on-data-broker-sales.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* London, UK: Profile Books.

Zweifel-Keegan, Cobun. 2024. "A view from DC: The beginning of the end of the free flow of data." International Association of Privacy Professionals, October 25. https://iapp.org/news/a/a-view-from-dc-the-beginning-of-the-end-of-the-free-flow-of-data/.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org