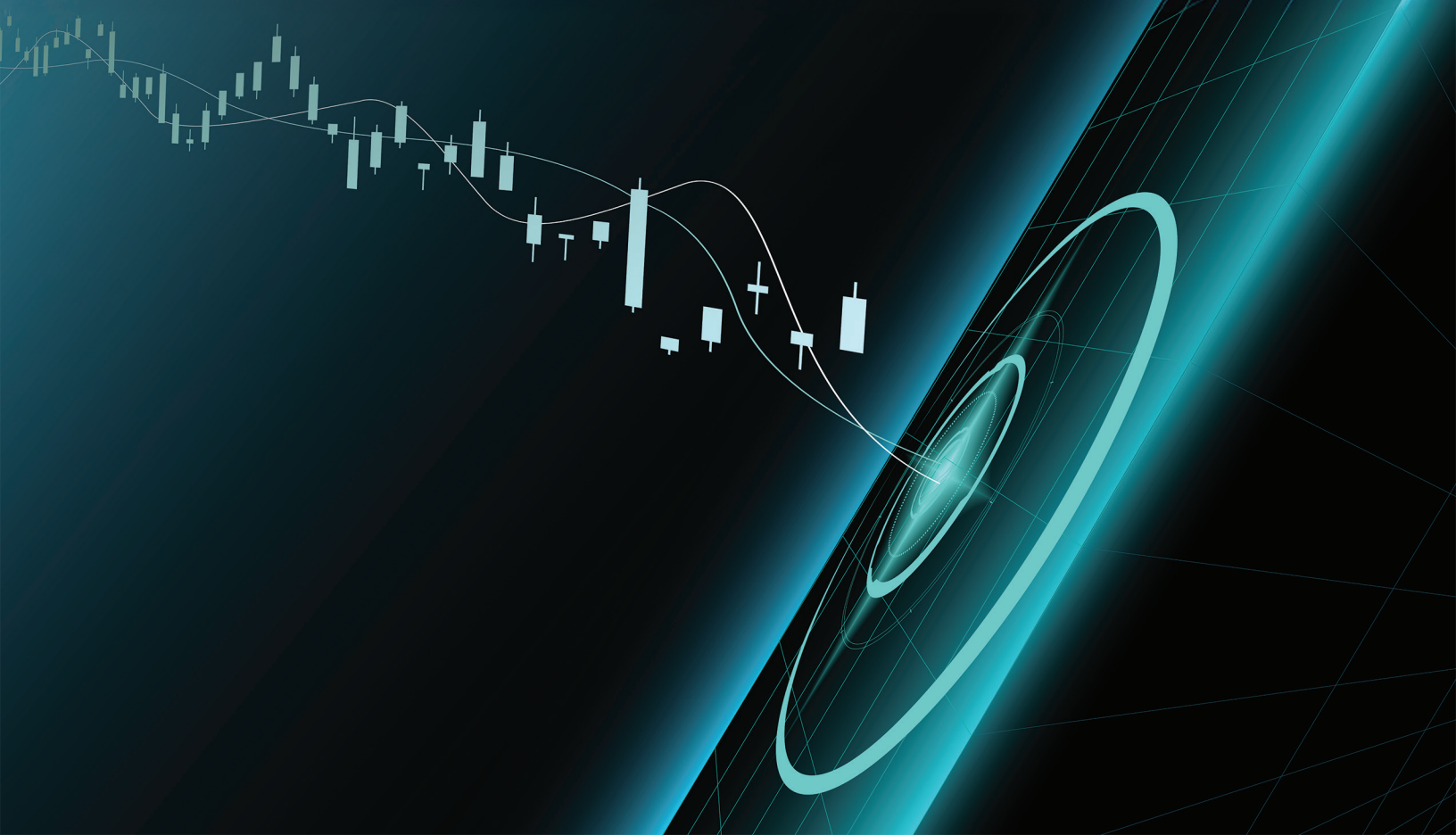
Centre for International
Governance Innovation

CIGI Papers No. 339 — November 2025

From NAFTA to Surveillance Capitalism

USMCA's Digital Order

Burcu Kilic



Centre for International
Governance Innovation

CIGI Papers No. 339 — November 2025

From NAFTA to Surveillance Capitalism
USMCA's Digital Order

Burcu Kilic

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

Senior Fellow S. Yash Kalash
Director, Program Management Dianna English
Senior Program Manager Jenny Thiel
Program Manager Grace Wright
Publications Editor Lynn Schellenberg
Manager, Publications Jennifer Goyder
Graphic Designer Sami Chouhdary

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

Table of Contents

About the Author

Burcu Kilic is a CIGI senior fellow and a scholar, strategist and expert in trade and technology policy. She is principal consultant at BKS Ventures, where she advises organizations across civil society, philanthropy and government. She also teaches technology policy and international affairs as a professorial lecturer at the Elliott School of International Affairs at George Washington University.

She held fellowships at the Carr-Ryan Center at the Harvard Kennedy School (2024–2025) and the Digital Civil Society Lab at Stanford University (2021–2022), focusing on technology, trade and rights.

She was the head of policy at Frontier Technology, a Minderoo Foundation initiative, where she led the foundation's strategy on emerging technologies and championed responsible, rights-based innovation. Prior to that, she directed the Digital Rights Program at Public Citizen, a non-profit consumer advocacy organization in Washington, DC, and also led their research on access to medicines.

Her influence in tech policy, intellectual property and trade underscores her commitment to policy entrepreneurship and rights-based advocacy. She champions collaborative civil society engagement, policy entrepreneurship and innovative policy development on a global scale. In 2015, she was recognized as one of the 300 Women Leaders in Global Health for her work on health and trade policy.

She holds a Ph.D. from Queen Mary University of London, along with LL.M. degrees in intellectual property law (Queen Mary) and information technology law (Stockholm University). She earned her law degree from Ankara University, Turkey.

Acronyms and Abbreviations

AI	artificial intelligence
APEC	Asia-Pacific Economic Cooperation
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
FTA	free trade agreement
FTC	Federal Trade Commission
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GDPR	General Data Protection Regulation
IP	intellectual property
IPEF	Indo-Pacific Economic Framework for Prosperity
JSI	Joint Statement Initiative
NAFTA	North American Free Trade Agreement
NSC	National Security Council
OECD	Organisation for Economic Co-operation and Development
OPC	Office of the Privacy Commissioner of Canada
PIPEDA	Personal Information Protection and Electronic Documents Act
SMEs	small and medium-sized enterprises
TiSA	Trade in Services Agreement
TPP	Trans-Pacific Partnership Agreement
USMCA	United States-Mexico-Canada Agreement
USTR	US Trade Representative
WTO	World Trade Organization

Executive Summary

In 1994, the North American Free Trade Agreement (NAFTA) laid the groundwork for today's neo-liberal global trade order. Three years later, the US government's Framework for Global Electronic Commerce enshrined minimal government intervention and industry self-regulation for the tech industry, principles that have since defined US digital trade policy, culminating in the digital chapter of the United States-Mexico-Canada Agreement (USMCA). The USMCA locks in commitments on cross-border data transfers, server location requirements, source code access, algorithmic transparency and platform liability, prioritizing platform power over regulatory autonomy.

Digital technologies, central to commerce, governance and daily life, also pose numerous challenges for privacy, autonomy, market concentration, fairness, discrimination, child protection and corporate power. Competition authorities, privacy regulators and worker advocates now question the surveillance capitalist business model, yet trade rules continue to reinforce and legitimize it. Technology policy is a key focus of the ongoing negotiations over tariffs reinstated when US President Donald Trump took office in January 2025, which has provided an opening for tech companies to cast tariffs as market-correcting mechanisms. The formal review of the USMCA scheduled for July 1, 2026, represents a critical inflection point.

This paper traces US digital trade policy from the Clinton-era vision of self-tech regulation to today's far-reaching digital trade framework. It reveals how current digital trade rules clash with contemporary economic and social priorities, as well as industrial policies, and warns negotiators that if North American trade is to deliver shared prosperity and technological development and protect worker well-being, digital trade should shift from embracing surveillance capitalism to restoring democratic accountability.

Introduction: The Day After Tariff Day

On April 2, 2025, designated as "Tariff Liberation Day," US President Donald Trump sent shockwaves through the global trading system by reinstating tariffs ranging from 10 percent to 49 percent applied to nearly every country. Tariffs were even extended to geographically uninhabited remote islands (Treisman 2025). Although tariff policy has long been a signature element of President Trump's broader trade agenda, this dramatic announcement marked a departure from the global trade system the United States had architected.

Trump's hardline position on tariffs is only one pillar of his broader trade agenda. He has consistently portrayed himself as a champion of American workers and economic renewal. Yet the tariffs alone cannot reverse decades of deindustrialization, nor can they empower American workers if US trade policy continues to ignore the deeper structural forces shaping today's digital economy, particularly the unchecked power of big tech companies and the digital transformation of labour and markets.

Upon returning to office in January 2025, Trump issued a memorandum on "America First Trade Policy" (The White House 2025a), directing the US Trade Representative (USTR) to review the impact of the USMCA on American workers. The report to the president on the policy was delivered the day after "Tariff Liberation Day," on April 3. The White House only released an executive summary of the report, in which chapter 4 focuses on renegotiating the USMCA (The White House 2025c). Notably, the summary makes no mention of the agreement's digital trade provisions — an unfortunate omission, given that the digital trade chapter, chapter 19, remains one of the USMCA's most controversial sections.[1] It has played a central role in consolidating the power of big tech, both abroad and within the United States.

A thorough review of the USMCA would acknowledge that its digital trade rules, rooted in the neo-liberal trade order of the 1990s, have helped entrench surveillance capitalism, undermined

1 See *United States-Mexico-Canada Agreement*, 29 January 2020, c 19 (entered into force 1 July 2020), online: <https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf>.

regulatory oversight and weakened transparency in artificial intelligence (AI), market competition and worker protections. If the Trump administration is serious about its commitment to workers, it must confront how surveillance-driven business models, enabled and reinforced by binding and enforceable trade rules, are reshaping power dynamics in the workplace and the global economy.

Against this backdrop, this paper provides a comprehensive analysis of the evolution of digital trade rules, tracing their origins to the Clinton administration's neo-liberal approach to deregulation, free markets and the self-regulation ethos of Silicon Valley. It examines how these early policy frameworks shaped the global trade regime and laid the foundation for today's surveillance-driven digital economy. The paper also discusses how tech companies have strategically shaped the shift from "digitally enabled commerce" to "trade in data," expanding protections for cross-border data flows and source code while cementing their corporate power across jurisdictions.

The paper scrutinizes the USMCA's digital trade provisions, demonstrating how they concentrate markets and reinforce monopolistic power, facilitate the surveillance and AI-driven management of workers, limit regulatory and democratic oversight, and undermine fair competition and market access for small businesses.

As the July 2026 USMCA review approaches, this paper argues that the digital trade chapter must be fundamentally revisited. A worker-first trade policy cannot succeed while the USMCA protects the infrastructure of surveillance capitalism. Reclaiming democratic oversight over data, technology and the digital economy is essential, not only for the United States but also for Canada, Mexico and the future of fair and accountable trade in North America.

The Beginning: Back to the 1990s

Every story has a beginning. Some might point to January 2017, the start of the first Trump administration, as the moment the story of digital trade officially began. After all, Trump's signature trade deal, the USMCA, was the first US free trade agreement (FTA) to include a dedicated digital trade chapter. It adopted the "digital trade" narrative, long championed by tech and trade lobbyists, rebranding e-commerce rules under the more ambitious and comprehensive label of "digital trade."

However, while Trump's inauguration in 2017 and the transformation of NAFTA into the USMCA marked a significant milestone in the evolution of digital trade from a secondary issue to a US policy priority, it was not the true beginning.

The story of digital trade actually dates back to the early 1990s, when the foundations of the neo-liberal trade order were established. This was the decade that saw the creation of the World Trade Organization (WTO), the negotiation of the NAFTA and the rise of the "Washington Consensus," a series of policies that embraced trade liberalization, deregulation and globalization as the cornerstones of economic progress (Serra and Stiglitz 2008).

NAFTA was the first US FTA with a broad scope, negotiated between countries at different levels of development. Talks began in June 1990 between the United States and Mexico, during George H. W. Bush's presidency. Canada joined later in February 1991. The Bush administration aimed to conclude the deal before the end of his first term, viewing NAFTA as a significant geopolitical and economic milestone (Martin and Hills 2028).

After losing the 1992 election, Bush handed off the agreement to Bill Clinton, who campaigned to reinvent the New Deal for an era of deindustrialization. However, once in office, he embraced neo-liberal policies, championing deindustrialization and deregulation (Resnikoff 2023). While the NAFTA negotiations were completed during the Bush administration, it was Clinton who had to secure congressional approval. Public opinion at the time was largely unfavourable; polls showed a majority of Americans opposed the deal, and it faced strong resistance from labour, consumer and environmental groups. Nevertheless, Clinton pushed NAFTA through Congress with more Republican votes than Democratic, undermining the labour-liberal coalition that had helped bring him to the White House (Lichtenstein 2018). He signed NAFTA in December 1993, and it went into effect in January 1994.

NAFTA was only the beginning of Clinton's transformation into a champion of the neo-liberal order. His presidency laid the foundations for

globalization with the creation of the WTO and the sweeping deregulation of key sectors, such as telecommunications and finance, which contributed directly or indirectly to the 2008 financial crisis. He declared the "end of big government," ushering in a period of spending cuts, deregulation and widening income inequality (Resnikof 2023).

Among all Clinton-era initiatives, the most significant policy for the digital economy was the Framework for Global Electronic Commerce (the Framework). Released on July 1, 1997, the Framework outlined the federal government's approach to online advertising, privacy and commercial surveillance of the internet, and quickly became a blueprint for domestic and international digital policy (The White House 1997).

Ira Magaziner, a long-time Clinton friend and adviser, spent some time in Silicon Valley, where he learned the technology sector's view of cyberspace as something separate from the rest of society, an exceptional place that did not follow society's rules. He took on those values. When he returned to Washington, he led the drafting process of the Framework, which built on that world view.[2] In an interview at the time, he made this perspective clear: "We thought the risks of governments intervening in ways that would impede the development opportunity were greater than our actions that might encourage it. I think the government has legitimate roles to play in the economy. But in an area like this, I think caution is best" (Magaziner, Cutter and Costa 1998).

In line with that thinking, the Framework was developed under intense industry lobbying and shaped by Silicon Valley elites and self-interested commercial interests through an anti-democratic process in which the public played a minimal role. Public consultation was essentially an afterthought. By the time the first draft was made publicly available, it had already become the ninth version, drafted in close coordination with industry elites well before it was posted online at the White House website (Crain 2021, 43–51).

Building on five core principles, the Framework laid the foundations for the administration's laissez-faire approach to regulation (Samuelson and Varian 2002). These principles were, in brief: "1. The private sector should lead"; "2. Governments should avoid undue restrictions on electronic commerce"; "3. Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce"; "4. Governments should recognize the unique qualities of the Internet"; and "5. Electronic commerce over the Internet should be facilitated on a global basis" (The White House 1997).

The Framework was accompanied by a presidential directive instructing "all Federal department and agency heads to review their policies that affect global electronic commerce and to make sure that they are consistent with the five core principles of this report" (Clinton 1997). It became clear that the Clinton administration would not only defer to the private sector on many areas of domestic policy but also advocate for US business interests in global markets. In that regard, Clinton directed the USTR to work with foreign governments to both "secure agreement within the next 12 months that all products and services delivered across the Internet will not be subject to tariffs and that all equipment from which the Internet is built will also not be subject to tariffs" and "enforce existing agreements and secure new agreements to make electronic commerce a seamless global marketplace. This will include enforcing provisions of the recently concluded World Trade Organization (WTO) Telecommunications Services Agreement; ensuring that product testing, certification, and approval processes do not unnecessarily restrict trade; ensuring that service providers have nondiscriminatory access to customers worldwide; and other measures that ensure a free flow of commerce" (Government Publishing Office 1997, 1008).

The Framework aligns with a larger neo-liberal agenda that is primarily shaped by the interests of US corporations. Much like NAFTA, the internet policy positions were crafted in close coordination with corporate stakeholders, often down to the last detail, while sidelining the interests of American workers, consumers and the broader public. The neo-liberal consensus narrowed the scope of debate to self-(non)regulation and market-driven policies, highlighting the role of FTAs and deregulation in advancing Silicon Valley's interests both in the United States and abroad (Crain 2021, 51–55).

2 See Harvard Carr-Ryan Center for Human Rights (2025).

Exporting Deregulation: The Framework Goes Global

The Framework called for private sector leadership in the development of internet commerce, explicitly rejecting government regulation in favour of self-regulation. This approach positioned the United States not only as the architect of the digital economy but also as the enforcer of a new trade order in which data flows freely, tech companies are shielded from liability and governments are discouraged from intervening in digital markets: "As we discussed this approach with others around the globe, with governments that tend to be more regulatory by instinct, we tried to explain it as a matter of practicality rather than ideology. It's not that we don't care about privacy; we do care very much, but we think this is a more effective way to enforce it. So, the simple answer to the question is: We think industry has the same motivation as regulators in this case; and we think that industry self-regulation is more effective given the nature of this medium" (Magaziner, Cutter and Costa 1998).

It did not take long for the Clinton administration's vision to gain international traction. Not long after, in 1998, the United States successfully shepherded the Asia-Pacific Economic Cooperation (APEC) Blueprint Action on Electronic commerce,[3] which established a regional policy framework for the development of electronic commerce in the region. Closely mirroring the Clinton administration's Framework, it reaffirmed private sector leadership, minimal regulation and a commitment to avoiding undue restrictions on e-commerce. This deregulatory approach shaped norms across the Asia-Pacific region for many years to come.

The same year, Clinton's agenda took centre stage globally. At the 1998 WTO ministerial meeting in Geneva, WTO members adopted the Declaration on Global Electronic Commerce (the Declaration), recognizing the "new opportunities for trade" in global electronic commerce. The Declaration instructed the General Council to "establish a comprehensive work programme to examine all trade-related issues relating to global electronic commerce, including those issues identified by Members" (Gao 2022).

One of these issues was the imposition of customs duties for digital services and content. The United States secured a temporary moratorium on customs duties on electronic transmissions, with a commitment that "members will continue their current practice of not imposing customs duties on electronic transmissions." The definition of "electronic transmissions" has remained undefined in the context of international trade rules since then, allowing the scope of the moratorium to expand with the digital economy. The moratorium prevented WTO members from imposing tariffs or adopting local revenue measures on digital content and services, and has limited their ability to experiment with industrial or fiscal policies (Kaukab 2024). The moratorium has been renewed at every WTO Ministerial since 1998, but there is growing opposition from developing countries, and its future became uncertain following the 2024 Ministerial deadlock (Farge and Uppal 2024).

E-commerce provisions began to appear in US FTAs as early as 2000, starting with the US-Jordan FTA. The accompanying joint statement on e-commerce declared that "Electronic Commerce will be the engine of economic growth in the twenty-first century" (Daley and Halaiqah 2000), explicitly endorsing the Clinton administration's e-commerce-first vision. Both parties committed to promoting a liberalized trade environment for electronic commerce, aimed at encouraging investment in new technologies and stimulating the innovative uses of networks to deliver products and services. In the FTA, Jordan pledged to refrain from imposing customs duties on electronic transmissions and avoid unnecessary barriers on electronic transmissions (Nsour 2003; The White House 2000). The US-Jordan FTA marked a significant milestone in integrating the 1997 Framework into the architecture of US trade policy, setting the stage for binding and enforceable digital trade chapters in future FTAs.

At the same time, the multilateral trading system was struggling to recover from the fallout of the 1999 WTO Ministerial in Seattle, which had exposed not only deep global divisions over trade liberalization but also growing domestic opposition to the global trade order (Engler 2019). It became clear that the benefits of neo-liberal

3 See the APEC Blueprint for Action on Electronic Commerce at www.apec.org/meeting-papers/leaders-declarations/1998/1998_aelm/apec_blueprint_for. The APEC ministers endorsed the documents of the blueprint in 1998 in Kuala Lumpur, Malaysia.

trade policies were unevenly distributed. As Paul R. Krugman and Maurice Obstfeld observe: "Owners of a country's abundant factors gain from trade, but owners of a country's scarce factors lose… compared with the rest of the world the United States is abundantly endowed with highly skilled labor and…low-skilled labor is correspondingly scarce. This means that international trade tends to make low-skilled workers in the United States worse off, not just temporarily, but on a sustained basis" (quoted in Autor, Dorn and Hanson 2016).

NAFTA's adverse effects began to materialize in the late 1990s, as economic studies started to show that expanding trade lowered the prices of import-competing goods and put downward pressure on the real wages for affected workers. For instance, manufacturing industries accounted for 78 percent of the net jobs lost under NAFTA, resulting in a total of 686,700 manufacturing job losses (Scott 2003). NAFTA has also contributed to rising income inequality and the declining relative wages of US workers without a college degree, who comprised 72.1 percent of the workforce in 2001 (Mishel, Gould and Shierholz 2012; Scott 2003).

Still, the George W. Bush administration played a leading role in advancing the neo-liberal trade order, ambitiously signing FTAs in nearly every corner of the world. Building on the WTO rules, the US FTAs pushed further by demanding deeper market liberalization, deregulation and stringent intellectual property (IP) rules that reinforced monopolistic control over knowledge, technology and medicines in exchange for preferential access to the US market (Erickson 2018).

Meanwhile, US internet and telecommunications companies were quietly building a new economic order: surveillance capitalism. This form of capitalism commercialized surveillance, turning personal data into a resource for predicting and manipulating human behaviour. It claims private human experience as a free source of raw material for the market dynamic, which is then translated into behavioural data. It began with Google's rollout of targeted advertising in 2001 and soon became the dominant business model of the tech industry, reshaping markets, governance and the global digital order (Zuboff 2019).

Following the US-Jordan FTA, e-commerce provisions became a regular feature of subsequent US FTAs, with each new FTA building on the previous one to gradually expand both the scope and enforceability of e-commerce rules. They evolved along two tracks: the first track incorporated existing WTO obligations, such as the moratorium on customs duties for electronic transmissions; the second track introduced new rules that went beyond existing WTO obligations, including consumer protection, cross-border data flows and electronic signatures (Gao 2018).

It took only a few years to evolve from a few e-commerce provisions to a dedicated e-commerce chapter. The US-Singapore FTA (2003) introduced the first standalone e-commerce chapter, highlighting the growing importance of the digital economy in US trade policy.

The Bush administration continued the Clinton administration's laissez-faire approach to tech regulation and particularly incubated and normalized the surveillance capabilities of Silicon Valley after the terrorist attacks of September 11, 2001. Yet, despite its interest in surveillance, the administration was largely absent from technology policy (McCullagh 2009), and the global interests of Silicon Valley never rose to the level of a trade priority. While the United States began including standalone e-commerce chapters in trade agreements during the Bush administration, the provisions mainly were non-binding "best effort" clauses rather than binding and enforceable commitments. Unlike Clinton's trade agenda, which explicitly positioned e-commerce as a US trade priority, the president's 2008 trade agenda made no mention of e-commerce at all (Office of the USTR 2008). Instead, Bush's trade policy focused heavily on IP enforcement and the expansion of copyright protections online, often prioritizing the interests of Hollywood studios and global media corporations, and setting the stage for an eventual clash with Silicon Valley over the future of the internet.

The tech companies did not have to wait for their own Silicon Valley president, who not only brought Silicon Valley to Washington but also became the most enthusiastic promoter of its interests globally. Under Barack Obama's administration, the interests of big tech moved to the centre of US trade policy, shaping trade negotiations around the world.

Consolidation: Embedding the Global E-commerce Agenda

The Clinton administration laid the foundation for the neo-liberal global trade order and the infrastructure of surveillance capitalism. From early on, the US government has embraced the rhetoric of "innovation," treating the American tech sector as uniquely exceptional, too dynamic for traditional regulation and best governed through self-regulation. Therefore, government actions that advanced capital expansion and profit making were reframed as non-regulatory or non-interventionist, preserving the illusion of laissez-faire governance (Crain 2021, 51).

While Silicon Valley was left unregulated at home, it needed protection against foreign governments' intervention and "overreach." The USTR emerged as a guardian of Silicon Valley companies' interests abroad, portraying foreign regulations as threats to both commerce and speech. Under the banner of promoting a "free and open internet," the USTR played a crucial role in helping US tech companies expand their surveillance business model abroad, shielding them from foreign regulatory scrutiny (Kilic 2025).

This approach reflected the broader logic of US trade policy under neo-liberalism: what is good for American corporations is good for America. Guided by this principle, the USTR has historically operated in close coordination with US multinationals, including those in manufacturing, pharmaceuticals, entertainment and so forth, aggressively pushing their agendas in foreign markets in exchange for preferential access to the US market. This strategy, known as linkage bargaining (Ryan 1998), enabled American multinational corporations to liberalize markets, deregulate, dismantle domestic protections and expand IP monopolies worldwide. While linkage bargaining delivered profits for corporate America, it left many American workers, communities and small businesses behind.

If the 1990s were the beginning, the Obama era marked the consolidation and peak of both the neo-liberal trade order and surveillance capitalism. President Obama was often described as Silicon Valley's president. During his term, American tech companies provided expertise, services, advice and even personnel to the administration, building a close partnership with the White House. They continued to enjoy a laissez-faire regulatory environment, substantially expanding and intensifying their lobbying presence, and quickly became influential power players in Washington's policy circles (Vaidhyanathan 2016).

Those were the years when the European Commission began entertaining the idea of strengthening digital privacy rights. The commission took steps to update and modernize the existing data protection rules and principles outlined in the Data Protection Directive 95/46/EC, which ultimately led to the development of the General Data Protection Regulation (GDPR). In response to these regulatory initiatives, viewed by many in Washington as discriminatory and trade-restrictive non-tariff barriers, tech companies began lobbying for their removal (Zuboff 2019). They adopted a new strategy, pushing for binding and enforceable rules that would pre-empt or constrain the foreign regulations that were beginning to emerge. This position, for instance, was clearly articulated in a Google Public Policy paper in 2010, which urged "policymakers in the United States, European Union, and elsewhere to take steps to break down barriers to free trade and Internet commerce. These issues present challenges, but also an opportunity for governments to align 21st century trade policy with the 21st century economy" (Boorstin 2010).

The Trans-Pacific Partnership Agreement: A New Chapter

It was no surprise, then, that Obama's flagship trade deal, the Trans-Pacific Partnership Agreement (TPP), included its binding and enforceable chapter 14 on e-commerce, advancing e-commerce rules that aligned with the interests of Silicon Valley.

The TPP was President Obama's signature economic initiative, involving 12 countries that represent roughly 12 percent of the world's population and 40 percent of global GDP (Williams 2013, 3). Launched in 2009 and concluded in late 2015, the TPP was the most ambitious trade

pact of the twenty-first century. It brought together countries with vastly different levels of development and diverse social, economic and political priorities: Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, Vietnam and the United States.

Of the TPP's 30 chapters, only five dealt with traditional trade issues such as tariffs, customs and trade remedies. The remaining chapters covered a variety of regulatory and legal issues, including IP, state-owned enterprises, financial services, e-commerce, investment, labour, pharmaceuticals and other issues that directly shape the lives of millions of people in the Pacific Rim.

Scholars, economists and other critics raised significant concerns throughout the negotiations about both the closed-door process, which lacked transparency and public input, and the content of the agreement (Stiglitz and Hersh 2015; Labonté, Schram and Ruckert 2016; Flynn 2012).

While much public attention focused on controversial provisions around IP and investment, e-commerce rules were central to the TPP's twenty-first-century model. Yet, they remained entirely secret throughout the negotiations. There was no public discussion or scrutiny. However, tech lobbyists consistently framed the e-commerce rules as setting high standards for the digital economy.

Between 2009 and 2015, hundreds of pages of draft TPP chapters were leaked; however, the full text of the e-commerce rules only became available once the final text of the agreement was released in December 2015.

The e-commerce chapter of the TPP was built on the provisions from previous US FTAs, yet its scope was far greater; the Office of the USTR (2015, 1) described the TPP as "the most ambitious and visionary Internet trade agreement ever attempted." It was the first trade deal to include binding rules on e-commerce. US trade negotiators persisted in removing trade barriers and establishing standard trade rules and disciplines in the Asia-Pacific Region to advance the interests of US tech companies.

The TPP rules are carefully designed to constrain governments' ability to regulate a rapidly changing digital environment in areas such as privacy, anti-competitive practices, AI policy, workers' rights, government data, cybersecurity, national security, and other human rights issues.

A deeper analysis of how these rules evolved and were incorporated into the USMCA, as well as how they continue to shape the regulatory landscape in North America, follows in the next section. However, to lay the groundwork, here are a few of the key provisions in the TPP:

- **Data free flow rules limiting domestic regulatory options:** The primary focus of the US tech industry's e-commerce agenda was to establish binding standards for the unrestricted flow of data across borders, as expressed, for example, in a submission to the USTR from Robert W. Hollyman,[4] then the president and CEO of the Business Software Alliance: "It is not sufficient merely to prevent barriers to electronic commerce and the provision of computer-related services. It is equally necessary to secure the freedom of transfer and exchange of data among data centers that are located in different TPP countries. Laws and regulations concerning data privacy and data security, for example, must not be permitted to prevent the flow of data across international boundaries" (Office of the USTR 2012). The TPP advanced this goal by liberalizing cross-border data flows while placing objective limits on how domestic privacy rules and regulations may interfere with parties' trade commitments. Although the provision includes an in-built trade exception, it is narrowly framed. Measures must achieve a "legitimate public policy" objective and must not be applied in an arbitrary or discriminatory manner, must not constitute a disguised restriction on trade and must not impose data-transfer restrictions "greater than are required to achieve the objective." This is an exceptionally difficult test to satisfy. WTO jurisprudence has rejected the same public policy defence in all but two of the 50 cases, effectively curbing governments' ability to introduce legitimate policy measures aimed at protecting consumers, the environment and other public interests (Rangel 2022).
- **Prohibition from placing any restriction on the location of computing facilities (or servers) and data processing:** The provision prohibits governments from requiring that data be stored and processed locally, regardless of whether such measures were intended to protect financial

4 Holleyman, appointed US Deputy Trade Representative by President Barack Obama in September 2014, later led the Digital Trade Working Group and the USTR's digital trade agenda known as the "Digital 2 Dozen."

data, safeguard health records, dismantle monopolistic digital entities or ensure national security. It does not distinguish between protectionist data localization mandates and narrowly tailored measures enacted for public policies. While the provision includes a public policy exception, as noted above, the threshold it imposes is high and has proven inadequate in practice to protect such measures under international trade rules.

- **Restrictions on access to source code:** The TPP set a precedent as the first FTA to prohibit governments from requiring the disclosure of source code as a prerequisite for the import, distribution, sale or use of software or products embedded with software. These restrictions on access and disclosure raise significant concerns about public oversight and accountability, effectively creating barriers to due process and regulatory scrutiny. By establishing exclusive IP protection over source code, with only narrow exceptions, the provision significantly limits the government's ability to examine, audit or assess the digital technologies.

The TPP marked the final chapter of neo-liberalism in the United States. By the time Obama signed it in January 2016, it had become increasingly disconnected from the prevailing political reality and the broader economy. The public sentiment was negative (Gallagher 2015). As the president sought congressional approval, it became clear that the neo-liberal trade agenda was losing favour. Key congressional leaders expressed skepticism about the far-reaching provisions (Calmes 2015) and never scheduled a vote on the agreement (Yuhas 2016).

Remarkably, both major presidential candidates in the 2016 election, Democrat Hillary Clinton (who had supported the early development of the TPP as Obama's Secretary of State) and Republican Donald Trump, opposed the deal on the campaign trail (Roberts and Felton 2016). Trade policy played a central role in the election, and Trump's aggressive stance on trade agreements possibly helped secure his path to the White House.

Immediately after taking office in 2017, President Trump announced that the United States would not enact the TPP, marking a departure from the Obama administration's extensive free-market agenda. Because the TPP required approval by countries representing a certain percentage of its market to take effect, Trump's move meant the accord could not be enacted among the remaining bloc.

The remaining TPP countries overcame this problem by establishing a "new" pact with a new name, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).[5] The CPTPP preserved nearly all of the original US-crafted rules but introduced a new mechanism for bringing it into force. Over the following years, these rules shaped the global trade landscape, including certain aspects of Trump's trade policies: the TPP's e-commerce chapter, carried forward into the CPTPP, quietly became the core of his digital trade agenda.

Rebranding: From E-commerce to Digital Trade

NAFTA has long been at the centre of debates about how trade agreements have harmed American workers, accelerated inequality and empowered American multinational corporations. For decades, progressives, unions, consumer groups and environmental advocates have consistently criticized NAFTA as the cornerstone of the neo-liberal trade order (Kaufman 2024).

Trump also repeatedly blamed NAFTA for the US trade deficit and the decline of American manufacturing jobs. He framed the agreement as a symbol of failed globalization and promised during his presidential campaign to either renegotiate it or withdraw from it entirely (Graham and Lawder 2017). Upon taking office, he was persuaded by Mexican and Canadian leaders to pursue renegotiation. In an effort to "modernize" this 24-year-old agreement, officials from the United States, Canada and Mexico negotiated a revised agreement in 2018. The outcome was the USMCA,[6] a rebranded NAFTA 2.0 that introduced targeted revisions and new

5 *Comprehensive and Progressive Agreement for Trans-Pacific Partnership*, 8 March 2018 (entered into force 30 December 2018), online: <www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cptpp-ptpgp/index.aspx>.

6 *United States-Mexico-Canada Agreement*, 29 January 2020 (entered into force 1 July 2020).

chapters. It preserved the structure and logic of NAFTA 1.0 and built upon the template established by subsequent US FTAs, including the TPP.

Although Trump's USMCA was built on the TPP and mirrored much of its text, it included more robust protections for workers. It moved away from some of the TPP's most controversial provisions, such as pharmaceutical patent protections. The USMCA served as a transitional agreement, building on the TPP while taking small steps to challenge specific neo-liberal trade provisions. Trump's former trade representative, Robert Lighthizer, argued that trade policy should prioritize raising wages and improving workers' well-being, rather than focus solely on benefits for markets (Lighthizer 2017).

The USMCA, however, included provisions on e-commerce that were even more extensive than those in the TPP. The USMCA negotiations took place under the radar, concluding quickly in closed-door meetings. This low-profile approach enabled tech companies to significantly influence the agreement, resulting in the USMCA containing provisions that heavily favoured the industry more than any previous agreement.

In fact, the USMCA included a new e-commerce chapter, "Digital Trade," which built on the TPP's e-commerce obligations by adding additional commitments and offering fewer exceptions to address public policy concerns. This presented a shift away from the e-commerce narrative, which carried echoes of the 1990s, toward a contemporary framework of digital trade poised to tackle digital protectionism (Chander 2018). The shift was driven, in part, by the tech industry's discontent with the "outdated" e-commerce narrative in the WTO, especially following their unsuccessful bid to secure a mandate for a new WTO agreement on e-commerce during the Eleventh WTO Ministerial Conference in Buenos Aires in 2017.

Despite broad bipartisan support for the USMCA, many US law makers were unaware that the agreement included sweeping digital trade provisions. At the time, digital policy remained a fringe issue for most members of the US Congress. It was 2018, the year of the Cambridge Analytica scandal, and Facebook's CEO Mark Zuckerberg was still insisting that AI would solve the platform's problems (Jeong 2018). The GDPR had just entered into force, and California had passed the Consumer Privacy Act. The tech industry was still claiming that both laws would "break the Internet or otherwise kill innovation" (Chander, Kaminski and McGeveran 2021, 1791), revealing how shallow and deflective the broader public debate over tech accountability was.

Proponents argued that binding rules reduce market fragmentation, lower compliance costs and promote innovation by guaranteeing legal certainty. They claimed that uniform standards across borders — though, in the case of the USMCA, this meant enshrining the lack of comprehensive privacy rules or other tech regulations — can help companies scale digital services without navigating divergent national privacy or data-localization regimes. In turn, this predictable legal environment attracts investment and fosters cross-border partnerships (Meltzer 2013).

Much of the public discussion surrounding the USMCA centred on headline issues, including pharmaceutical patent protections, investor-state dispute settlement and worker protections. These were the issues where advocacy efforts and political attention were heavily focused. Tech companies and their lobbyists were able to push through the digital trade chapter with no scrutiny or resistance. Canada and Mexico, having already agreed to similar provisions under the CPTPP, did not approach the e-commerce chapter as controversial and therefore did not prioritize the e-commerce negotiations. A few voices in Canada raised concerns about data flows, privacy and trade secret protections (Scassa 2018; Geist 2018), but Canadian negotiators largely set these concerns aside.

As a result, the USMCA, the only US agreement with such digital commitments approved by Congress, adopted some of the most far-reaching digital trade rules ever seen in a trade agreement.

These provisions quickly became a tech industry wish list for every future trade negotiation. Some provisions were so far-reaching and restrictive of regulatory flexibility that even the Trump administration's USTR had to later walk back elements of them in subsequent negotiations.

The USMCA's digital trade chapter, chapter 19, was notably comprehensive. While it built on the TPP, it went even further in scope and ambition. The TPP started to shift the focus from digitally enabled commerce to the broader and more complex domain of trade in data. Electronic commerce, understood as the digitally enabled trade of physical goods and services (for example, ordering a book online) or their digital equivalents (purchasing

an e-book), largely aligns with the existing rules under the WTO framework. However, trade in *data* represents a less established paradigm (Alschner 2023). It raises new economic, political and normative challenges, from protecting personal privacy to safeguarding worker protections and preserving domestic regulatory policy space.

Preserving domestic regulatory policy space became a key concern in the years that followed, as the unchecked power of tech companies faced increased scrutiny. With growing demands for accountability and responsibility in the digital economy, and an increasing need to protect American workers, consumers and everyday people, as well as to give small and medium-sized enterprises (SMEs) a fair shot, more people started to question the digital trade rules. Tech lobbyists were no longer able to promote the narrative that what was good for big tech was good for America.

These questions become more pronounced under President Joe Biden's administration, which took a more critical view of big tech's business model. The administration adopted a whole-of-government approach to competition (The White House 2021), aligning trade and competition policies in a proactive and consistent manner, particularly in the context of the digital economy. The focus shifted toward enhancing resilience and curbing excess market concentration. As antitrust policy expanded beyond solely focusing on consumer welfare to broader considerations of fairness, non-discrimination and recognition of workers' rights, US trade policy evolved accordingly. A new worker-centred trade agenda emerged (Baltzan 2023), putting the interests of workers at the centre of policy making and asking a fundamental question: Who really benefits from today's trade rules?

Big tech's "winner-takes-most" digital trade rules have failed to deliver benefits to workers and SMEs, either domestically or internationally. Despite the tech industry's claims of job creation, innovation and economic growth, these rules supported market concentration at home, empowered tech companies abroad and contributed to the global expansion of the surveillance capitalist order. Rather than promoting broad-based prosperity and offering fair opportunities to SMEs, the digital trade agenda has too often reinforced market concentration and undermined democratic oversight.

In October 2023, the USTR withdrew its support for some controversial digital trade proposals at the WTO's Joint Statement Initiative (JSI) negotiations, which involved 90 nations in Geneva (Lawder 2023). Though surprising to many, the move was in line with the Biden administration's broader agenda to curb big tech influence and reassert democratic governance in trade policy making. The administration could no longer overlook the surveillance capitalist business model of tech companies, nor could it continue to empower them in trade agreements that preserve this model.

In the words of USTR Katherine Tai in November 2023, in a video by Bloomberg (2023), "The cross-cutting nature of these issues means that if we're going to lead using trade rules at a time when there is no consensus but massive amounts of debate and questioning, then I as USTR am committing massive malpractice and probably committing policy suicide by getting out ahead of all of the other conversations and decisions that we need to make as a country."

The USTR's announcement received both praise and criticism from members of Congress, civil society groups, think tanks, digital rights organizations and the tech industry. Notably, the criticism was louder, highlighting the contentious nature of the policy change and big tech's wide influence across politics, academia and civil society.

As of 2025, under the second Trump administration, the United States appears to be reverting to old standards. The *2025 National Trade Estimate* report identified several data protection and competition regulations as non-tariff trade barriers (Office of the USTR 2025), signalling the revival of the old playbook. At the same time, non-tariff barriers have become a key part of ongoing tariff negotiations (The White House 2025b) and, reportedly, the USTR is urging governments to make digital trade commitments in these negotiations (Renshaw 2025). Canada's decision at the end of June to withdraw its digital services tax (a requirement of its Digital Services Tax Act) after Trump threatened to halt all tariff negotiations underscores the stakes involved (Mukherjee and Chiacu 2025). Tech companies have successfully reframed tariffs as market-correcting mechanisms designed to penalize distortive practices and level the global regulatory playing field. They placed what they termed non-tariff barriers at the centre of Trump's trade diplomacy, making them a central part of negotiations.

It is far from clear how a tech-first trade approach would benefit American workers. Trump campaigned as the champion of American workers,

and early in his term directed the USTR to evaluate the USMCA's impact on workers (The White House 2025a). It is hard to see how a tech-first trade policy that reinforces the surveillance capitalist business model aligns with an "America First" vision. Given the historical record of past trade agreements for US workers and communities, the key question is how digital trade rules can be designed to support broader economic renewal and shared prosperity in North America.

If the Trump administration is genuinely committed to workers, it must recognize how surveillance capitalism shapes the workplace, deepening the power imbalance between workers and tech companies, and how trade agreements reinforce this model.

To better understand these dynamics, the following section provides a closer examination of the digital trade chapter in the USMCA. It analyzes key provisions that illustrate how the agreement prioritizes the interests of US big tech companies, often at the expense of workers, competition, regulatory autonomy and fair market access.

USMCA Deep Dive

As noted, the USMCA's chapter 19 on digital trade has a broad scope, including provisions that facilitate digitally enabled commerce as well as those governing trade in data. Since today's tech business model is built on unrestricted data collection and monetization, this section focuses on the most prominent and widely discussed provisions related to data governance and their broader implications for workers, competition, regulatory oversight and economic fairness.

Data Free Flow Rules Limiting Domestic Regulatory Space

On cross-border transfer of information by electronic means, the USMCA stipulates that:

> 1. 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.
>
> 2. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure:
>
> (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
>
> (b) does not impose restrictions on transfers of information greater than are necessary *to achieve the objective* [emphasis added].[5] (Article 19.11)

Footnote 5 reads: "A measure does not meet the conditions of this paragraph if it accords different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party" (ibid.).

This provision builds on the TPP article 14.11,[7] "Cross Border Transfer of Information by Electronic Means," but it adopts a notably different framing. The TPP text starts with a recognition that "each Party may have its own regulatory requirements concerning the transfer of information by electronic means." This acknowledgment carries no legal weight. The core trade obligation remains that parties "shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person." While parties may have their own regulatory requirements, they are still required to allow cross-border data flows, unless their measures qualify under the narrow conditions of trade exceptions.

In fact, trade obligations often come with trade exceptions, allowing flexibility for public policy measures. For instance, in the case of data free flows, the obligation is clear as "each Party shall allow the cross-border transfer of information by electronic means" in the TPP, as noted above, and "no party shall prohibit or restrict the cross-border transfer of information, including personal information" in the USMCA (article 19.11). Both obligations are straightforward, but the USMCA

7 See in full at *Trans-Pacific Partnership Agreement*, 4 February 2016, online: USTR.gov: <https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf>.

language goes further by explicitly banning restrictions, thereby strengthening the obligation.

Trade Exception

The challenge lies in crafting an exception language that strikes a balance between these firm obligations and the flexibility needed to pursue public measures. In this context, the issue is not simply the flow of data, particularly personal data, across borders, but the broader implications of unrestricted data flows on privacy, competition, protection of children and workers' rights, among others. Since the early days of the TPP, trade negotiators have struggled to develop exceptions to address this challenge.

Trade exceptions, by design, limit the extent to which domestic regulations can interfere with trade commitments. The USMCA exception, for instance, is more restrictive compared to the TPP, which is already limited in scope and effectiveness. Both the USMCA (article 19.11.2) and the TPP (article 14.11.3) exceptions require a public policy measure to achieve a "legitimate public policy objective," which is not self-defining. It is not clear what can qualify as a legitimate public policy objective; a party would need to defend the legitimacy of a public policy objective in the event of a dispute. This ambiguity makes it difficult for governments to justify regulatory measures, such as privacy or competition laws, as legitimate trade exceptions. For instance, new regulations, especially those not widely adopted, such as platform regulation, could be seen as creating a non-tariff trade barrier by increasing operational complexity and costs for businesses (see Computer & Communications Industry Association 2024).

The USMCA requires that any exception to data free flow obligations be justified as "necessary." This means that a party should demonstrate not only that the measure is effective in achieving its public policy goal, but also that no less trade-restrictive measure could achieve the same objective. This creates a significant burden. The party may be required to demonstrate that a broad range of less trade-restrictive regulatory options would be insufficient.

After the necessity is established, the inquiry continues. The measure must also not constitute either "a disguised restriction on trade" or an "arbitrary or unjustifiable discrimination" (article 19.11.2(a)). These standards invite scrutiny of the motives and intentions of the country defending a measure and further raise the bar for defending public interest measures under trade law.

As mentioned above, although framed differently, the exceptions in both the USMCA and the TPP borrow from the general exceptions clause of the WTO agreements, specifically the General Agreement on Tariffs and Trade (GATT), article XX,[8] and the General Agreement on Trade in Services (GATS), article XIV.[9] The GATT exception requires a policy measure to be necessary to achieve a specific public policy objective and not to constitute arbitrary or unjustifiable discrimination or a disguised restriction on international trade. Historically, the WTO tribunals have interpreted these exceptions narrowly. Out of 48 cases where the general exception was invoked, a mere two were successfully upheld (Rangel 2022).

This posed a significant challenge for the Biden administration's trade officials. The digital trade commitments in the USMCA were not aligned with US domestic priorities. They took away all the policy space available to US regulators and law makers to address issues such as privacy, antitrust, workers' rights and platform accountability. During the Indo-Pacific Economic Framework for Prosperity (IPEF) negotiations, the USTR reportedly sought to introduce more flexible exceptions to provide greater policy space. It is speculated that the IPEF proposal revisited the TPP exception with tweaks such as shifting the burden of proof and adding a footnote for flexibility in transfers to non-parties (Fortnam 2023).

While these efforts were significant, they fell short of addressing the core issue. The classic paradigm of trade rulemaking, which hinges on meeting stringent trade exceptions to preserve regulatory policy space, led USTR negotiators into the complex realities of digital governance. This is a domain where Americans expect the government to protect their rights and regulations, and where the executive branch looks to Congress for guidance on governance. In this context, the USTR's efforts did not meet the expectations of Congress and the American public. Recognizing the limitations of applying conventional trade frameworks to data

8 General Agreement on Tariffs and Trade, 15 April 1994, 1867 UNTS 187, 33 ILM 1153 (entered into force 1 January 1995), art XX, online: <www.wto.org/english/res_e/booksp_e/gatt_ai_e/art20_e.pdf>.

9 *General Agreement on Trade in Services*, 15 April 1994 (entered into force 1 January 1995), online: <www.wto.org/english/docs_e/legal_e/gats_e.htm>.

governance and emerging technologies, the USTR chose not to take the lead but instead stepped aside, creating space for Congress and the administration to directly shape digital policy (Kilic 2024a).

Following the USTR's decision to step aside, the US Chamber of Commerce (2023) and several industry groups escalated the issue to the National Security Council (NSC), warning that the move would allow China to shape global digital norms — although there is little evidence that China aims to establish a comprehensive rulebook for the digital economy comparable to US trade policy in the last 30 years. In response, the NSC launched a stakeholder consultation process in November 2023, bringing together tech companies, trade associations, academics, labour unions and civil society groups (Kuttner 2023). This was followed by an interagency process involving the USTR, the State Department, the Department of Commerce, the Federal Trade Commission (FTC), the Department of Labor and other agencies to develop new digital trade positions and draft exceptions that would not constrain domestic policy space (Kuttner 2024).Despite holding near-weekly meetings through May 2024, the agencies were unable to reach a consensus. In the end, even the US government's top trade lawyers were unable to craft language that preserved the policy space necessary to address domestic policy priorities.

Europe's Dilemma

The exception language has long created challenges in trade negotiations. It was one of the key reasons the Trade in Services Agreement (TiSA), a plurilateral trade initiative liberalizing global services, collapsed in 2016. TiSA was another agreement negotiated during the Obama administration. The negotiators made good progress over the three-plus years of negotiations, but the negotiations ultimately stalled because the parties could not agree on an exception language flexible enough to accommodate the European Union's red line on privacy. US and EU negotiators failed to reach a deal (Stupp 2016) before the election of President Trump, and the agreement was quietly shelved.

The TiSA negotiations started a deeper conversation within the European Union about the implications of data free flows. At that time, studies confirmed what many EU negotiators had not wanted to accept: the general exceptions in the GATS, which they had hoped would safeguard privacy, were insufficient to safeguard the privacy and data protection rights of European citizens (Bennett and Raab 2006). More recent research highlighted that the GDPR might not pass the WTO's general exception test on several particular grounds, including the existence of less trade-restrictive measures (Irion, Yakovleva and Bartl 2016). The GDPR, for instance, which was enacted later and is known for its strict rules on data collection, processing, storage and usage, has been criticized for being overly burdensome and tedious.

It became clear that data free flow provisions granted businesses freedom to transfer, use, process and monetize data (including personal information) as they saw fit, without being subject to regulatory restrictions. More importantly, these provisions allowed data to be transferred across borders without verifying whether the receiving country provided adequate protection for the rights and freedoms of individuals. In practice, the location of data often determines the legal rules governing its use. Since most US tech companies store their data in the United States, US law governs the use, storage, processing and transfer. But at the time — and still today — there was no comprehensive federal data protection law in the United States. As a result, European privacy rules could not guarantee that the personal data transferred to the United States would be processed fairly and lawfully, or only for specified and legitimate purposes.

Without jurisdiction over where and how data is handled, it becomes impossible to verify whether the data is retained longer than is necessary or for the purposes for which it is processed, or used for unauthorized AI training, whether it is monetized or not. Nor is it clear what rights individuals have in the event of unauthorized or unlawful processing, or accidental loss, destruction or damage to personal data.

At its core, the contemporary data free flow provisions raised many questions without satisfactory answers. European negotiators have long struggled to safeguard the European Union's robust data protection standards, particularly the GDPR, in trade agreements. In 2018, the European Union introduced "horizontal provisions"[10] on cross-border data flows and privacy, creating a self-standing exception design to preserve regulatory autonomy for fundamental rights, independent

10 Horizontal provisions require the European Union to consider certain social values in all its actions and policies (Giudici 2024).

of WTO-style legal tests and qualifiers (European Commission 2018). These horizontal provisions were incorporated into FTAs with Chile and New Zealand.

However, tensions emerged in negotiations with the United Kingdom, which opposed the European Union's horizontal approach and favoured limiting the impact of privacy regulations on cross-border data transfers (Fahey and Mancini 2023). The parties reached a compromise deal, suggesting that the European Union may be willing to show flexibility in the wording of data flows provisions. Most recently, the European Union and Japan agreed on new language, replacing the rendezvous clause in their 2018 FTA, which postponed negotiations on data flows to a later date (European Commission 2023). The revised text blends elements of the European Union's horizontal provisions with an exception in the style of the CPTPP. It effectively reintroduces the WTO's legal tests and qualifiers and reduces the policy space provided by the horizontal provisions. The European Data Protection Supervisor questioned the purpose, timing and necessity of this new language (European Data Protection Supervisor 2024).

It is worth noting that horizontal provisions never received broad support and have been subject to fierce criticism from the tech industry. Industry groups have argued that the European Union's interests would be better protected under the existing GATS rules and exemptions (DIGITALEUROPE 2018).

Personal Information Protection

The USMCA's data free flow provision (article 19.11) is often linked to the agreement's provision on the protection of personal information (article 19.8.2), which requires parties to adopt or maintain a domestic legal framework that safeguards the personal information of the users of digital trade. Many interpret article 19.8 as a sign of strong privacy protection in trade agreements. While article 19.8 is long and appears comprehensive, its impact is limited. It requires domestic protection frameworks to follow the principles and guidelines of relevant international bodies such as the Organisation for Economic Co-operation and Development (OECD) and the APEC Privacy Framework. But there is a footnote within article 19.8.2 that undercuts the strength of the provision by allowing parties (the United States) to comply through non-binding mechanisms: "For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy."

The United States lacks a comprehensive federal data protection law. Instead, it relies on a patchwork system of federal and state laws and regulations, sector-specific regulations, the enforcement authority of the FTC and industry self-regulation. These fragmented and often voluntary measures fall short of providing robust privacy protections. Since much of the world's data flows to the United States, the USMCA's provision on personal information protection offers little in meaningful safeguards for personal data. It does not oblige the United States to introduce a comprehensive privacy or data protection framework.

Chilling Effect

While trade negotiators continue to search for language that balances policy space with data free flow provisions, the tech industry is taking full advantage of having these provisions in trade agreements.

By way of illustration, in 2019, shortly after Canada signed the USMCA (referred to in Canada as CUSMA), the Office of the Privacy Commissioner of Canada (OPC) considered revising its policy on transborder data flows under the Personal Information Protection and Electronic Documents Act (PIPEDA). The OPC wanted to introduce a requirement for express or implied consent for cross-border data transfers, depending on the sensitivity of data and the reasonable expectations of the individual. The OPC framed this as a "risk of harm" assessment, requiring express consent where there is a "meaningful risk that a residual risk of harm will materialize and will be significant" (OPC 2019a). It argued that the general rule under PIPEDA, which requires organizations to obtain consent for the collection, use or disclosure of personal data, should also apply to cross-border data transfers. In this context, organizations would be required to provide individuals with "clear information" about disclosures to third parties, including recipients outside of Canada, and the associated risks of such disclosures. They would also need to inform individuals of any alternatives should they choose not to consent, unless the cross-border transfer is "integral to the delivery of a service" (ibid.).

The proposal received clear pushback from the tech industry and allies. Critics questioned how the proposed consent regime would coexist with Canada's international trade obligations, which generally prohibit regulatory measures that could be seen as disguised restrictions on trade (the so-called "non-tariff trade barriers"). Some argued that a US company could challenge the requirement before a trade tribunal (Thompson 2019).

The US industry groups claimed that the proposal was incompatible with Canada's commitments under both the USMCA and the TPP:

> Considerations contained in the OPC's discussion document, and the OPC's proposed consumer consent requirement for cross-border data transfers, are inconsistent with the obligations provided in the Canada-U.S.-Mexico Agreement (CUSMA), which prohibits restrictions on cross-border data flows that are greater than necessary to achieve legitimate public policy objectives. CUSMA also states that parties must ensure that "any restrictions on cross-border flows of personal information are necessary and proportionate" to the risk. Building on App Association views above, we believe that the OPC's proposed consumer consent requirement for cross border data transfers goes beyond the scope of being "necessary to achieve a legitimate public policy interest." Similarly, the OPC's proposed approach very likely runs afoul of similar obligations in the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP). (The App Association 2019, 3–4)

The OPC ultimately withdrew its proposal and decided to maintain the status quo until the law is changed (OPC 2019b).

Interestingly, Montana's Genetic Information Privacy Act of 2023[11] includes a similar consent requirement for international data flows. The act defines "genetic data" broadly to include raw sequence data, genotypic and phenotypic information and self-reported health information. It establishes comprehensive requirements for notice, use and consent for companies processing consumer genetic data (Lynch 2023).

The act's section 4.7 includes an explicit restriction prohibiting the storage of genetic data in any country currently sanctioned by the US Department of the Treasuries' Office of Foreign Assets Control or designated as a foreign adversary under Title 15 of the US Code of Federal Regulations (section 7.4(a)).

Section 4.7 also states that "genetic data or biometric data of Montana residents collected in the state may only be transferred or stored outside the United States with the consent of the resident." This consent requirement is similar to what the OPC once proposed, but ultimately abandoned, under pressure. It is unclear whether the trade exception discussed above would preserve Montana's — or any other US state's — ability to implement and enforce such policies. In this sense, USMCA's article 19.11 not only threatens to undermine Canada's privacy law but also constrains the ability of the US Congress and individual states to protect privacy and regulate data flows.

Geopolitics of Data Free Flows

While discussions around data free flows often centre on privacy and data protection, the issue extends far beyond these concerns. Data free flow provisions give companies broad discretion over how they collect, use and monetize data. This flexibility has lately become a concern for US policy makers, as China has emerged as the leading destination for global data flows. A 2020 investigation by the Japanese Nikkei index found that 23 percent of the world's data flowed to China, twice the size of the data in the United States (Uematsu and Tsunashima 2020). This shift raised alarm bells in Washington, as Chinese tech companies, including not only TikTok but also Shein, Temu, AliExpress and others, have rapidly expanded their US market share and influence over the last few years.

There are also significant implications for AI, as data is now widely recognized as a core component of AI infrastructure (Bietti 2025). AI technologies require the processing of massive volumes of data for training and operation. AI systems also rely heavily on other data-intensive cross-border activities, such as cloud computing services. The more data a company collects, the more effectively it can train and optimize its AI models. Today, much of the data for AI is collected and monetized

11 *Genetic Information Privacy Act*, Mont Code Ann tit 30 ch 23 pt 1 (2023), online: <https://archive.legmt.gov/bills/2023/BillPdf/SB0351.pdf>.

by a small group of powerful corporations controlling every corner of our digital lives. In the United States, market concentration has become a significant concern, prompting a coordinated effort to enhance resilience and address excessive market concentration across digital markets. Policy makers and regulators are increasingly recognizing that trade agreements play a structural role in shaping both domestic and digital governance, particularly in regulating data flows and, by extension, the development and deployment of AI.

In recent years, US antitrust law and enforcement have undergone a major transformation. The focus has moved away from a pro-corporate efficiency paradigm toward actively challenging concentrated corporate power. This shift extended across multiple policy areas through an "all-of-government" approach. After two decades of inaction, antitrust regulators under the Biden administration, and now under the Trump administration, started to advance a more assertive and democratized vision of antitrust. This new vision frames antitrust as a broader public effort to pursue the interests of workers, small businesses and farmers, not just American consumers (Caffara and Kilic 2024).

It also reflects a strong recognition that free trade has not always served the interests of people and has often functioned as a tool that extends corporate power and shapes global markets in ways that benefit monopolist corporations, rather than one promoting pro-worker or democratic outcomes.

As awareness of the consequences of free trade policies over the past 30 years increases, concerns about digital trade and data free flows are becoming central to every dimension of social and economic policy in the digital economy. They start with privacy, but extend to the protection of children, workers' rights, the concentration of power, AI infrastructure, industrial policy and job creation. In this new landscape, countries must be aware of the policy space they have available to them.

Even for the United States, where data flows freely today, there is no guarantee it will remain the primary destination. In the near future, US data may increasingly flow to China or to privately governed "data havens," similar to tax havens, where it can be stored, processed, monetized and used to train AI systems beyond the reach of accountability and democratic governance.

If we are to put workers at the centre of trade policy, we must ensure that digital trade rules do not undermine governments' ability to protect labour rights, regulate data practices and shape AI and digital markets in ways that promote equity, prosperity and democratic governance. Trade policy must not pre-empt the very tools needed to secure a just digital economy.

Prohibition from Placing Any Restriction on the Location of Computing Facilities

Article 19.12 of the USMCA, regarding location of computing facilities, states that "no Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."

This provision generally targets measures that require the local storage or processing of data, commonly referred to as "data localization." This term has often been marginalized in trade discussions, framed as a protectionist policy rather than a legitimate regulatory measure.

The provision is closely linked to the data free flow provision discussed above. Provisions of this nature often conflate forced data localization with legitimate regulatory measures intended to safeguard privacy, financial data and the broader public interest. This confusion risks framing key governance tools as "non-tariff barriers" and undermines governments' ability to regulate the digital economy.

"Data localization" lacks a universally accepted definition and has historically been associated with China, where its policy on data localization is widely regarded as a protectionist strategy. Initially, the term was broadly applied to any measure influencing the location of data storage. However, as global discussions have matured, more targeted definitions have emerged. In recent discussions, data localization often refers specifically to the explicit requirement for data to be stored or processed or both within the confines of a domestic territory (López González, Casalini and Porras 2022)

Not all "data localization" measures are created equal; context, intent, and governance structures matter (see Figure 1). Countries adopt very different approaches depending on the policy goals they seek to advance, such as national security, regulatory oversight, economic development

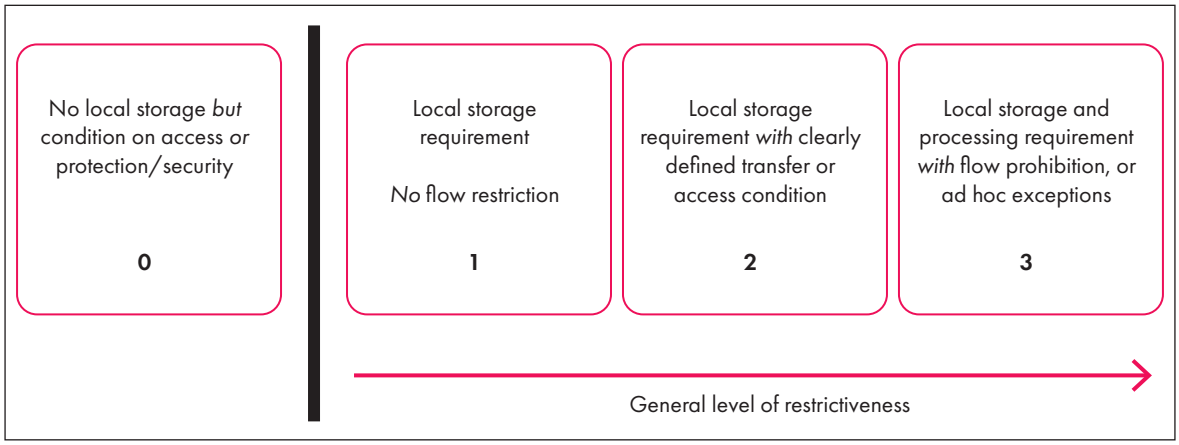
or digital sovereignty. The measures differ based on the sectors they target, for instance, health-related measures differ from election-related measures in terms of the type of data involved, the scope of the measure and so on.

Broadly speaking, data localization frameworks can be grouped into three main categories, which may not be clearcut. The least restrictive category requires that a copy of the data be stored domestically but does not also prohibit its storage and processing abroad. This requirement is often intended to provide access for domestic regulators, rather than to claim control over data flows. A well-known example of this approach is Kenya. Under its Data Protection (General) Regulations, personal data linked to the strategic interests of Kenya, which include facilitating the conduct of elections, public health, early childhood education and public finance, must either be processed through servers located in Kenya or have at least one copy stored in a data centre within the country.[12]

Kenya's experience during the 2017 presidential elections illustrates the rationale behind this type of measure. The Kenyan election commission had contracted a French technology firm to manage its digital election infrastructure, including servers hosted overseas. When the Supreme Court ordered the electoral commission to provide access to election data during the legal proceeding disputing election results, the commission was unable to do so, citing its lack of control over the foreign servers. The court annulled the election, in part due to the failure to provide access to election data and the lack of transparency. In response, Kenya's data protection laws were updated to enhance transparency and accountability, particularly in the electoral process, requiring a copy of the data to be held in the country. Doing so ensured that if future disputes arise, Kenyan courts can easily access the necessary data directly, without relying on foreign intermediaries or navigating complex cross-border access barriers (Ndonji 2021).

The second category builds on the first category and requires a copy of the data to be stored within the country, but permits its transmission abroad under clearly defined conditions, such as user consent or necessity. The Australian My Health Records Act requires that health record

Figure 1: Not All Data Localization Measures Are Created Equal



Source: López González, Casalini and Porras (2022, 7).
Note: This is an adaptation of an original work by the OECD, which notes: "Figure is schematic; elements do not singularly identify any given country's approach to data localization. Different approaches tend to apply to different types of data, even within the same jurisdiction." The opinions expressed and arguments employed in this adaptation should not be reported as representing the official views of the OECD or of its member countries.

12 *The Data Protection (General) Regulations* (Kenya), 14 February 2022, s 26, online at: <www.odpc.go.ke/wp-content/uploads/2024/03/THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021-1.pdf>.

information be stored in Australia so that Australian authorities have access and oversight. However, it allows overseas access, when necessary, for instance by individuals (the data subjects) or by registered health-care providers operating overseas(López González, Casalini and Porras 2022).

The third and last category, according to OECD classification, imposes strict controls over data. It mandates that data be stored and processed exclusively within the country, while restricting its transfer abroad. These types of measures typically apply to issues related to national security or the protection of critical infrastructure, where the government seeks to maintain complete control over sensitive data to prevent foreign access, influence or dependency. The Cybersecurity Law of the People's Republic of China, for instance, mandates that critical information infrastructure operators store essential data within the country, thereby reinforcing the government's ability to monitor and secure data it considers essential (ibid.).

This USMCA provision adopts a blanket prohibition. It fails to distinguish between different types of measures, instead broadly targeting any measure related to the location of data. Unlike the TPP version, it also eliminates exception language. It creates an absolute commitment with no public policy exceptions — even though such exceptions often fail to provide meaningful public policy safeguards in practice. This has far-reaching implications for countries that enact regulations to safeguard personal or financial data, protect national security or curb the power of monopolistic digital platforms.

In recent years, the United States has introduced a growing number of policies at both the federal and state levels that require local storage and processing of data. At the federal level, these measures reflect a shift toward prioritizing data security, national sovereignty and privacy. In 2024, for instance, Congress passed the Protecting Americans' Data from Foreign Adversaries Act,[13] which prohibits data brokers from transferring specific categories of sensitive personal information offshore.

At the state level, Montana's Genetic Information Privacy Act prohibits the storage of genetic and biometric data collected in the state in any country sanctioned by the US federal government. Similarly, California's Confidentiality of Medical Information Act requires that sensitive medical information be stored in the state and prohibits its transfer or storage outside California.[14]

Yet, it is essential to recognize that not all these measures are created equal. Some function as essential regulatory tools to enforce data protection laws, uphold democratic accountability and ensure that data remains available for public oversight, investigation or redress. The Montana and California laws exemplify how local storage or processing measures can serve legitimate public interest objectives. The absence of even a narrow exception in the USMCA for such measures reflects a trade-first approach in which commercial interests override domestic regulatory autonomy. This imbalance raises serious concerns about the shrinking policy space for public policies, particularly at a time when oversight over data is increasingly central to labour rights, fundamental freedoms, market fairness and democracy.

Restrictions on Access to Source Code (and Algorithms)

On source code, the USMCA says:

> 1. No Party shall require the transfer of, or access to, a source code of software owned by a person of another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.
>
> 2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination enforcement action, or judicial proceeding,[6] subject to safeguards against unauthorized disclosure. [Footnote 6 says, "This disclosure shall

13 US, Bill HR 7520, *Protecting Americans' Data from Foreign Adversaries Act of 2024*, 118th Cong, 2024, online: <www.congress.gov/bill/118th-congress/house-bill/7520/text>.

14 US, AB 352, *An act to amend Sections 56.101 and 56.108 of, and to add Section 56.110 to, the Civil Code, and to amend Section 130290 of the Health and Safety Code, relating to health information*, 2023–2024, Reg Sess, Cal, 2023, online: <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB352>.

not be construed to negatively affect the software source code's status as a trade secret, if such status is claimed by the trade secret owner."] (Article 19.16)

The TPP set a precedent as the first FTA to prohibit the governments from requiring the disclosure of source code as a condition for the import, distribution, sale or use of software or products containing that software. The USMCA has expanded this restriction to include algorithms, further extending the limitations to disclosure, transfer and access.

These limitations raise serious concerns about public oversight and democratic accountability, effectively placing key aspects of software and algorithmic systems beyond the reach of regulatory scrutiny. The provision provides for an exclusive IP right over source code and algorithms, with only narrow exceptions.

Although the language of article 19.16 expands the scope of the exception to regulators for specific investigations, enforcement actions and judicial proceedings, the core problem remains unresolved. The structure of the provision effectively enshrines trade secret protection at the expense of regulatory oversight.

This dynamic has significant implications for the governance of AI. When these companies assert trade secret protection over their algorithms, training data, input parameters or any aggregated data, they effectively create a "legal black box" (Kilic 2024b). This raises a critical question: Does the trade secret protection claimed by these companies inevitably lead to the denial of due process rights for individuals or corporations (Coglianese 2023)? When the broadened and strengthened scope of trade secrets is factored into this equation, the problem becomes even more complex and opaque. This highlights the tension between proprietary protection in AI systems and the fundamental right to due process. A comprehensive and multifaceted response is needed to address the advancements in AI and the intricacies of trade secrets law.

One of the most pressing concerns is that these provisions restrict governments from conducting even basic *ex ante* screenings of AI systems. Such reviews are crucial for identifying algorithmic discrimination, labour law violations, competition risks and biases inherent in public-facing technologies. Without access to the underlying code and algorithms, regulators are forced to rely on voluntary disclosures or black box testing, which fail to ensure meaningful accountability (Jones et al. 2024).

This limitation is especially problematic in high-stakes domains such as employment, credit scoring, social benefits and criminal justice, where decisions made by opaque systems can have far-reaching consequences for workers, patients, communities or individuals. It also weakens the role of non-state actors, such as labour unions, civil society organizations, consumer safety advocates and researchers, who are increasingly involved in algorithmic oversight. For instance, in the Netherlands, the SyRI (System Risk Indication) algorithm was used by the government to detect welfare fraud, but it disproportionately targeted low-income and migrant communities. Civil society groups successfully challenged the system, but only after a lengthy legal battle and sustained advocacy efforts, which ultimately enabled the public to access algorithms. Algorithmic transparency provided a solid foundation for identifying violations of the right to privacy in the system. AI systems challenge traditional concepts of transparency and accountability, while simultaneously reinforcing the need for radical transparency regarding the impact of AI systems in the information environment (Rachovitsa and Johann 2022).

Radical transparency is critical in the workplace, where every action is surveilled and catalogued, AI systems are deeply integrated, and algorithms dictate hiring, shift allocation, performance evaluations, pay and even termination. Amazon warehouse workers, for instance, have raised concerns about automated systems that track productivity in real time and, in some cases, initiate termination without supervisory discretion (Kantor, Weise and Ashford 2021). The digital transformation of the workplace demands entirely new categories of rights, privacy and protection.

If source code and algorithms are shielded by trade agreements, labour unions and worker advocates may be unable to audit these systems, identify discriminatory practices or pursue redress through collective bargaining or legal challenge. Algorithmic opacity poses a direct threat to labour rights, undermining due process, workplace fairness and the ability to challenge harmful or unjust management practices.

The asymmetry created by these kinds of provisions exacerbates power imbalances between tech companies and public authorities. Shielding AI systems, whether through algorithms or training data, as trade secrets tends to overly prioritize commercial interests, thereby creating barriers to due process. When algorithms or data sets are protected as trade secrets, there is an increased risk that they might reinforce existing biases and inequalities, leading to the emergence of a "techno-social divide." This divide essentially creates a barrier to accessing information, with profound implications for privacy, democracy, workers' rights, competition and social justice. It calls for continued efforts, comprehensive strategies and more rigorous legal frameworks to ensure that the deployment of AI systems does not compromise transparency, accountability or due process.

Since the TPP, subsequent trade agreements have refined and expanded exceptions to better reflect the current state of technology. Yet, as technology continues to evolve, these efforts consistently fall short. For instance, the limited exceptions introduced in the USMCA in 2018 were extended in the US-Japan Digital Trade Agreement in 2019, which removed USMCA's narrow restriction that allowed source code and algorithms to be made available only to regulatory bodies.[15] While this adjustment represents progress, it addresses only a small part of the broader problem.

It remains unclear whether the provision in the US-Japan agreement permits regulators to require the transfer of source code and algorithms in other legitimate contexts, for example, as a condition of approving a merger or acquisition, for environmental regulation, including climate-related measures, or under a compulsory licensing scheme during an emergency. Without explicit flexibility for such scenarios, these provisions risk undermining the government's ability to regulate in the public interest.

There is a growing recognition that such provisions risk hardcoding a deregulatory logic into the global digital economy and constraining the very tools governments need to ensure fairness, transparency and accountability in the age of AI. These concerns were central to the Biden administration's decision to withdraw US support for the source code provision in the WTO JSI, whose language closely mirrored the restrictive terms found in the USMCA. As with the parallel debate over exceptions to data free flow provisions, efforts within the NSC were unsuccessful in reaching a consensus. This once again underscored the challenge of introducing public interest exceptions to address the growing challenges of extensive trade secret protection. Rather than locking in these standards at the international level, trade negotiators should take their lead from domestic policy frameworks, incorporating exceptions established in national law and regulatory practice to preserve policy space for effective digital governance.

Platform Liability

The USMCA's provision on interactive computer services (article 19.17) states:

> 1. The Parties recognize the importance of the promotion of interactive computer services, including for small and medium-sized enterprises, as vital to the growth of digital trade.
>
> 2. To that end, other than as provided in paragraph 4, no Party shall adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created, or developed the information.
>
> 3. No Party shall impose liability on a supplier or user of an interactive computer service on account of:
>
> (a) any action voluntarily taken in good faith by the supplier or user to restrict access to or availability of material that is accessible or available through its supply or use of the interactive computer services and that the supplier or user considers to be harmful or objectionable; or

15 "This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of the other Party to preserve and make available the source code of software, or an algorithm expressed in that source code, for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure." *Agreement Between the United States of America and Japan Concerning Digital Trade* (7 October 2019), art 17, online: <https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf>.

(b) any action taken to enable or make available the technical means that enable an information content provider or other persons to restrict access to material that it considers to be harmful or objectionable.

4. Nothing in this Article shall:

(a) apply to any measure of a Party pertaining to intellectual property, including measures addressing liability for intellectual property infringement; or

(b) be construed to enlarge or diminish a Party's ability to protect or enforce an intellectual property right; or

(c) be construed to prevent:

(i) a Party from enforcing any criminal law; or

(ii) a supplier or user of an interactive computer service from complying with a specific, lawful order of a law enforcement authority.

5. This Article is subject to Annex 19-A.

The USMCA is also the first US trade agreement that requires trading partners to adopt provisions modelled on Section 230 of the Communications Decency Act. The provision shields interactive computer service providers from liability for third-party content published on their platforms, building on the core protections of Section 230.

Section 230, which grants broad immunity to online platforms from liability for user-generated content, has become one of the most contentious issues in US tech policy, drawing criticism from both sides of the political aisle. While Republicans have accused tech companies of censoring conservative voices, Democrats have argued that platforms have failed to adequately address misinformation, hate speech and other online harms. Advocates passionately argue for and against it, indicating a deeply polarized environment.

This provision became a flashpoint in the final stages of the USMCA talks between the White House and House leadership. There were concerted efforts, including by House Speaker Nancy Pelosi, some of her top deputies and several Republican members, to remove the provision from the final deal. These efforts ultimately failed,[16] and the language remained intact (Liu 2022).

The inclusion of Section 230-style protections in the USMCA was a major victory for the tech industry, which also succeeded in reinforcing the same language in the US-Japan Digital Trade Agreement. The provision not only exports the liability shield to other jurisdictions but also complicates efforts to revisit the liability domestically. By embedding Section 230's core principles into a binding and enforceable trade agreement, the provision now enjoys an additional layer of insulation that potentially chills future legislative efforts to regulate platform accountability (McGill 2019).

However, it soon became clear to the USTR after the USMCA that these Section 230 protections embedded in the USMCA cannot be easily replicated in future trade agreements. Navigating away from this provision in the IPEF was particularly challenging. Early in those negotiations, the USTR recognized that such a politically contentious clause in the US proposals was not feasible. Despite intense industry lobbying and pressure to preserve the liability shield as a trade priority, these efforts failed to shift the administration's position. The USTR formally withdrew the proposal in 2023, ahead of its broader decision to withdraw support for other continuous digital trade provisions discussed above in the WTO's JSI. This move marked a significant shift, acknowledging the complex domestic and political landscape surrounding digital trade. It reflected a broad effort to align trade negotiations with evolving national priorities and bipartisan debates over platform accountability.

The USMCA Review: Reset or Replay?

The USMCA is scheduled for its first formal joint review on July 1, 2026, as laid out in article 34.7. This six-year review offers parties an opportunity to assess the agreement's performance, recommend revisions and

16 Commenting on this, Speaker Pelosi regretted that she was too late to address it: "I lost – they had 230 in the agreement, there are some members that wanted that…it's a real gift to big tech" (cited in Mills Rodrigo 2019).

determine whether to extend the agreement beyond its default expiration date in 2036.

The text of the article provides only broad procedural guidance, leaving the precise structure and negotiation dynamics of the review undefined. As the architect of the review clause, the United States is expected to play a central role in driving any proposed changes. Its internal policy review is scheduled for 2025, with public consultations set to begin as early as October 2025 (Bond et al. 2024).

Against this backdrop, the review raises broader political questions. Will the US trade negotiators press for meaningful oversight of the tech surveillance capitalist business model or reaffirm the status quo? And do Canada and Mexico have the appetite and leverage to demand stronger labour protections, data governance safeguards and accountability?

The Trump administration has been vocal about putting "American workers and families first." Its entire trade agenda centres on restoring prosperity to the working class, farmers and small businesses. The upcoming USMCA review presents a critical test: Will the Trump administration's "workers first" rhetoric translate into a meaningful assessment of the USMCA's digital trade chapter?

There is reason to be skeptical. The USMCA's digital trade rules, crafted to advance big tech's interest, represent the height of a neo-liberal surveillance capitalist order that goes back to the Clinton administration. These rules were built on outdated assumptions about free data flows, the tech industry's self-(non)regulation and a lack of transparency and accountability. They are increasingly misaligned with the realities of American workers, who now navigate a digital economy characterized by constant surveillance, targeted advertising, algorithmic decision making and eroding job security and protections.

Instead of empowering workers, these provisions tie the hands of regulators, hindering their ability to address algorithmic discrimination, exploitative workplace technologies, market concentration and the unchecked power of dominant tech firms. In sectors from warehouses to ride sharing, workers are monitored, evaluated and disciplined by opaque systems they cannot question, built on data they cannot access and governed by agreements they cannot influence.

There is limited public awareness of the depth and implications of these provisions. The expansion of digital trade rules has occurred with minimal debate outside industry circles. Civil society, labour unions, worker groups and academic experts have rarely been meaningfully included in negotiations, despite the provisions' potential to undercut rights and protections in multiple domains.

While the neo-liberal trade order, launched by NAFTA, sought to deliver economic growth and shared prosperity, many US communities instead experienced significant job losses, industrial decline and a concentration of economic power. Global trade policies have expanded Americans' access to low-cost imports but often at the expense of their domestic manufacturing jobs, economic security and the resilience of local industries.

The digital economy risks repeating the policy failures of the past. In today's economy, data is one of the most valuable assets, shaping not only markets but also every aspect of daily life. Surveillance is now deeply embedded in workplaces, homes, schools and the broader economic infrastructure. At this moment, it is critical not to repeat the mistakes of the 1990s, when neo-liberal trade rules and Silicon Valley's self-regulation theory were sold as engines of innovation and prosperity. The digital trade provisions of the USMCA reflect the same outdated vision, rooted in the same deregulatory mindset that trusts markets to deliver better outcomes, scales back antitrust enforcement and tolerates rising inequality as the price of growth. But that market promise of improved economic outcomes never materialized, unless one counts the sharp rise in corporate consolidation and wealth inequality over the past three decades.

Trump's "America first" approach naturally targets one of the most critical sectors of today and the future: AI. Facing an ongoing AI arms race with China, the Trump administration has adopted an increasingly protectionist stance on AI policy. It frames foreign tech regulations, whether they be about AI safety, competition or privacy, as "unfair" trade barriers. These so-called non-tariff barriers became a prime target for tariff negotiations. Even the European Union, once proud of introducing the first comprehensive AI regulation, is now considering delaying its implementation (Pollet and Haeck 2024).

On this side of the Atlantic, there is little appetite to regulate AI. A proposed moratorium, which would have introduced a 10-year ban on states' abilities to regulate AI, was stripped from the Trump administration's "Big Beautiful Bill" at the eleventh hour in the Senate (Morgan and Shepardson 2025). But that removal does not signal a shift toward AI oversight: neither the current administration nor Congress has any intention of regulating AI.

Canada has echoed the same reluctance. Canada's first AI minister stated that "the United States and China have no desire to buy into any constraint or regulation," and following their lead, pledged to "move away from 'over-indexing on warnings and regulation'" so the economy can fully benefit from AI (quoted in Karadeglija 2025).

In an environment where every country races to harness AI innovation with minimal oversight, predicting what the USMCA review will bring in terms of digital policy is challenging. Of course, forecasting any trade-related development in 2025 is a complex task. Far from a simple update, this review could rewrite the digital trade chapter or even shake the very foundations of the USMCA.

Regardless of what unfolds, restoring democratic oversight and economic justice demands a significant revision of the USMCA's digital trade chapter. The current provisions are not only ill-suited for the United States; they also erode essential regulatory space and undermine the public interest in Canada and Mexico. For the future of all three North American economies, it is essential to learn from past policy failures and move beyond the illusion of digital trade exceptionalism toward a framework that prioritizes the interests of North American workers, strengthens communities and safeguards democratic governance in the digital age.

Works Cited

Alschner, Wolfgang. 2023. "E-Commerce or Digital Trade? Why the Difference Should Matter To Trade Lawyers." Preprint, Social Science Research Network, January 11. https://doi.org/10.2139/ssrn.4321743.

Autor, David H., David Dorn and Gordon H. Hanson. 2016. "The China Shock: Learning from Labor Market Adjustment to Large Changes in Trade." Working Paper No. 21906. Cambridge, MA: National Bureau of Economic Research. https://doi.org/10.3386/w21906.

Baltzan, Elizabeth. 2023. "Worker-Centered Trade Policy, Peace, and Prosperity." Washington, DC: USTR Archives. https://ustr.gov/about-us/policy-offices/press-office/blogs-and-op-eds/2023/worker-centered-trade-policy-peace-and-prosperity.

Bennett, Colin J. and Charles Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, MA: The MIT Press.

Bietti, Elettra. 2025. "Data is Infrastructure." Preprint, Social Science Research Network, January 26. https://doi.org/10.2139/ssrn.5041965.

Bloomberg. 2023. "US, Taiwan Making Excellent Progress on Trade: Katherine Tai." December 7. Bloomberg Markets: The Close video, 07:33. www.bloomberg.com/news/videos/2023-12-07/us-taiwan-making-excellent-progress-on-trade-tai-video.

Bond, David E., Gregory Spak,Francisco de Rosenzweig, Carlos Véjar, Karen Luna and Ian Saccomanno. 2024. "North America Prepares for 2026 USMCA Review and Potential Renegotiation." White & Case LLP, November 14. www.whitecase.com/insight-alert/north-america-prepares-2026-usmca-review-and-potential-renegotiation.

Boorstin, Bob. 2010. "Promoting Free Trade for the Internet Economy." *Google Public Policy* (blog), November 15. https://publicpolicy.googleblog.com/2010/11/promoting-free-trade-for-internet.html.

Caffara, Cristina and Burcu Kilic. 2024. "Re-joining trade with antitrust." Centre for Economic Policy Research, March 7. https://cepr.org/voxeu/columns/re-joining-trade-antitrust.

Calmes, Jackie. 2015. "Trans-Pacific Partnership Is Reached, but Faces Scrutiny in Congress." *The New York Times*, October 5. www.nytimes.com/2015/10/06/business/trans-pacific-partnership-trade-deal-is-reached.html.

Chander, Anupam. 2018. "The Coming North American Digital Trade Zone." Council on Foreign Relations, October 9. www.cfr.org/blog/coming-north-american-digital-trade-zone.

Chander, Anupam, Margot E. Kaminski and William McGeveran. 2021. "Catalyzing Privacy Law." *Minnesota Law Review* 105: 1733–801. https://minnesotalawreview.org/article/catalyzing-privacy-law/.

Clinton, William J. 1997. "Remarks Announcing the Electronic Commerce Initiative." July 1. UC Santa Barbara, The American Presidency Project. www.presidency.ucsb.edu/documents/remarks-announcing-the-electronic-commerce-initiative.

Coglianese, Cary. 2023. "AI, Due Process, and Trade Secrets." *The Regulatory Review*, September 4. www.theregreview.org/2023/09/04/coglianese-ai-due-process-and-trade-secrets/.

Computer & Communications Industry Association. 2024. "CCIA Digital Trade Barriers in the European Union Two-Pager." February 5. https://ccianet.org/library/ccia-digital-trade-barriers-in-the-european-union-two-pager/.

Crain, Matthew. 2021. *Profit over Privacy: How Surveillance Advertising Conquered the Internet*. Minneapolis, MN: University of Minnesota Press. https://doi.org/10.5749/j.ctv20zbktm.

Daley, William M. and Mohammed Halaiqah. 2000. "U.S.-Jordan Joint Statement on Electronic Commerce." October. United States and Hashemite Kingdom of Jordan. www.sice.oas.org/Trade/us-jrd/St.Ecomm.pdf.

DIGITALEUROPE. 2018. "DIGITALEUROPE Comments on European Commission's Draft Provisions for Cross-Border Data Flows." May 3. Brussels, Belgium: DIGITALEUROPE. www.digitaleurope.org/resources/digitaleurope-comments-on-european-commissions-draft-provisions-for-cross-border-data-flows/.

Engler, Mark. 2019. "The Seattle Protests Showed Another World Is Possible." *The Nation*, November 29. www.thenation.com/article/archive/seattle-wto-protests/.

Erickson, Amanda. 2018. "How George H.W. Bush pushed the United States to embrace free trade." *The Washington Post*, December 2. www.washingtonpost.com/world/2018/12/02/how-george-hw-bush-pushed-united-states-embrace-free-trade/.

European Commission. 2018. "Horizontal provisions for cross-border data flows and for personal data protection (*in EU trade and investment agreements*)." News item, May 18. https://ec.europa.eu/newsroom/just/items/627665/en.

———. 2023. "EU and Japan conclude landmark deal on cross-border data flows at High-Level Economic Dialogue." Press release, October 27. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5378.

European Data Protection Supervisor. 2024. "Opinion 3/2024 on the signing and conclusion on behalf of the European Union, of the Protocol amending the Agreement between the European Union and Japan for an Economic Partnership regarding free flow of data." Brussels, Belgium: European Data Protection Supervisor. https://privacy-web.nl/wp-content/uploads/po_assets/925681.pdf.

Fahey, Elaine and Isabella Mancini. 2023. "Cross-border Data Flows between the EU, Japan and the UK: A Triangular Relationship." *Keio Law Journal* 49 (3): 61–69. https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=AA1203413X-20230330-0061.

Farge, Emma and Rachna Uppal. 2024. "WTO fails on major reforms, extends digital tariff ban in Abu Dhabi meeting." Reuters, March 1. www.reuters.com/business/wto-issues-new-draft-trade-deals-after-all-night-talks-some-issues-unresolved-2024-03-01/.

Flynn, Sean. 2012. "Law Professors Call for Trans-Pacific Partnership (TPP) Transparency." *InfoJustice* (blog), May 9. https://infojustice.org/archives/21137.

Fortnam, Brett. 2023. "In Bali, USTR to table revamped IPEF digital trade text, potential RRM." Inside US Trade, March 8. https://insidetrade.com/daily-news/bali-ustr-table-revamped-CCIA-digital-trade-text-potential-rrm.

Gallagher, Kevin P. 2015. "Saving Obama from a Bad Trade Deal." The American Prospect, March 4. https://prospect.org/2015/03/04/saving-obama-bad-trade-deal/.

Gao, Henry. 2018. "Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation." *Legal Issues of Economic Integration* 45 (1): 47–70. https://doi.org/10.54648/leie2018003.

———. 2022. "E-commerce Governance: Back to Geneva?" Global Cooperation on Digital Governance and the Geoeconomics of New Technologies in a Multi-polar World Essay Series, Centre for International Governance Innovation, February 14. www.cigionline.org/articles/e-commerce-governance-back-to-geneva/.

Geist, Michael. 2018. "Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards." In *Data Governance in the Digital Age*, 99–103. Waterloo, ON: CIGI. www.cigionline.org/publications/data-governance-digital-age/.

Government Publishing Office. 1997. "Memorandum on Electronic Commerce." July 7. *Weekly Compilation of Presidential Documents* 33 (27): 1006–10. www.govinfo.gov/content/pkg/WCPD-1997-07-07/html/WCPD-1997-07-07-Pg1006-2.htm.

Graham, Dave and David Lawder. 2017. "Grim reality of NAFTA talks sets in after tough U.S. demands." Reuters, October 14. www.reuters.com/article/business/grim-reality-of-nafta-talks-sets-in-after-tough-us-demands-idUSKBN1CK02F/.

Giudici, Silvia. 2024. "Interpreting EU Internal Market Powers in Light of Article 9 TFEU Social Objectives: Implications for the Attribution of Competences." *Croatian Yearbook of European Law and Policy* 20 (December): 31–57. www.cyelp.com/index.php/cyelp/article/view/579.

Harvard Carr-Ryan Center for Human Rights. 2025. "The United States of Surveillance Capitalism vs. The Rule of Law: How Far Will They Go?" YouTube video, 1:29:16. www.youtube.com/watch?v=bHzY1uQ5BuI.

Irion, Kristina, Svetlana Yakovleva and Marija Bartl. 2016. "Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements." Preprint, Social Science Research Network, November 30. https://doi.org/10.2139/ssrn.2877166.

Jeong, Sarah. 2018. "AI is an excuse for Facebook to keep messing up." *The Verge*, April 13. www.theverge.com/2018/4/13/17235042/facebook-mark-zuckerberg-ai-artificial-intelligence-excuse-congress-hearings.

Jones, Emily, Philippa Collins, Henning Grosse Ruse-Khan, Albert Sanchez-Graells, Kristina Irion, Cosmina Dorobantu, Burcu Kilic and Daria Onitiu. 2024. "AI Governance and the Future of Digital Trade Policy." Preprint, Social Science Research Network, December 4. https://doi.org/10.2139/ssrn.4987769.

Kantor, Jodi, Karen Weise and Grace Ashford. 2021. "The Amazon That Customers Don't See." *The New York Times*, June 15. www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html.

Karadeglija, Anja. 2025. "AI minister says focus is more on economic benefits, less on regulation." Global News, June 10. https://globalnews.ca/news/11234071/canada-ai-minister-economic-benefit-less-regulation/.

Kaufman, Dan. 2024. "How NAFTA Broke American Politics." *The New York Times*, September 3. www.nytimes.com/2024/09/03/magazine/nafta-tarriffs-economy-trump-kamala-harris.html.

Kaukab, Rashid S. 2024. "WTO Moratorium on Customs Duties on Electronic Transmissions." International Institute for Sustainable Development, October 30. www.iisd.org/articles/policy-analysis/wto-moratorium-customs-duties-electronic-transmission.

Kilic, Burcu. 2024a. "As Global Trade Goes Digital, Trust Becomes Critical." Opinion, Centre for International Governance Innovation, February 29. www.cigionline.org/articles/as-global-trade-goes-digital-trust-becomes-critical/.

———. 2024b. *Into Uncharted Waters: Trade Secrets Law in the AI Era*. CIGI Paper No. 295. Waterloo, ON: CIGI. www.cigionline.org/publications/into-uncharted-waters-trade-secrets-law-in-the-ai-era/.

———. 2025. "American Workers vs. Surveillance Capitalism: The Future of Digital Trade Policy." *Notes from the New Frontier of Power* (blog series), February 10. www.hks.harvard.edu/centers/carr-ryan/our-work/carr-ryan-commentary/american-workers-vs-surveillance-capitalism-future.

Kuttner, Robert. 2023. "Google's China Policy: How the National Security Council is trying to take over regulation of global data flows on the basis of what's good for Big Tech." The American Prospect, November 28. https://prospect.org/power/2023-11-28-googles-china-policy/.

———. 2024. "The Trade War Within the U.S. Government." The American Prospect, April 3. https://prospect.org/blogs-and-newsletters/tap/2024-04-03-trade-war-within-us-government/.

Labonté, Ronald, Ashley Schram and Arne Ruckert. 2016. "The Trans-Pacific Partnership: Is It Everything We Feared for Health?" *International Journal of Health Policy and Management* 5 (8): 487–96. https://doi.org/10.15171/ijhpm.2016.41.

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/.

Lichtenstein, Nelson. 2018. "A Fabulous Failure: Clinton's 1990s and the Origins of Our Times." *The American Prospect*, January 29. www.reuters.com/world/us/us-drops-digital-trade-demands-wto-allow-room-stronger-tech-regulation-2023-10-25/.

Lighthizer, Robert. 2017. "U.S. Trade Policy Priorities: Robert Lighthizer, United States Trade Representative." Transcript, September 18. Washington, DC: Center for Strategic and International Studies. www.csis.org/analysis/us-trade-policy-priorities-robert-lighthizer-united-states-trade-representative.

Liu, Han-Wei. 2022. "Exporting the First Amendment through Trade: The Global 'Constitutional Moment' for Online Platform Liability." Preprint, Social Science Research Network, March 21. https://doi.org/10.2139/ssrn.4059650.

López González, Javier, Francesca Casalini and Juan Porras. 2022. "A Preliminary Mapping of Data Localisation Measures." OECD Trade Policy Paper No. 262. Paris, France: OECD. https://doi.org/10.1787/c5ca3fed-en.

Lynch, Jennifer. 2023. "Montana's New Genetic Privacy Law Caps Off Ten Years of Innovative State Privacy Protections." Electronic Frontier Foundation, September 5. www.eff.org/deeplinks/2023/08/montanas-new-genetic-privacy-law-caps-ten-years-innovative-state-privacy.

Magaziner, Ira C., Ann Grier Cutter and Len A. Costa. 1998. "The Framework for Global Electronic Commerce: A Policy Perspective." *Journal of International* Affairs 51 (2): 527–38. www.jstor.org/stable/24357514.

Martin, Rachel and Carla Anderson Hills. 2018. "Remembering Bush 41: How Has NAFTA Shaped The Global Economy?" NPR, December 3. www.npr.org/2018/12/03/672836578/remembering-bush-41-how-has-nafta-shaped-the-global-economy.

McCullagh, Declan. 2009. "Bush leaves behind a mixed technology legacy." CNET, January 19. www.cnet.com/tech/tech-industry/bush-leaves-behind-a-mixed-technology-legacy/.

McGill, Margaret Harding. 2019. "Pelosi loses push to strip tech liability shield from USMCA." Axios, December 10. www.axios.com/2019/12/10/pelosi-loses-push-to-strip-tech-liability-shield-from-usmca.

Meltzer, Joshua. 2013. "The Internet, Cross-Border Data Flows and International Trade." *Issues in Technology Innovation*, No. 22. Washington, DC: Center for Technology Innovation at Brookings. www.brookings.edu/wp-content/uploads/2016/06/internet-data-and-trade-meltzer.pdf.

Mills Rodrigo, Chris. 2019. "Tech legal shield included in USMCA despite late Pelosi push." *The Hill*, December 10. https://thehill.com/policy/technology/473905-tech-legal-shield- included-in-usmca-despite-late-pelosi-push?rl=1.

Mishel, Josh Bivens, Elise Gould and Heidi Shierholz. 2012. *The State of Working America*. Twefth ed. An Economic Policy Institute Book. Ithaca, NY: Cornell University Press.

Morgan, David and David Shepardson. 2025. "US Senate strikes AI regulation ban from Trump megabill." Reuters, July 1. www.reuters.com/legal/government/us-senate-strikes-ai-regulation-ban-trump-megabill-2025-07-01/.

Mukherjee, Promit and Doina Chiacu. 2025. "U.S., Canada to resume trade talks after Ottawa drops digital tax." Reuters, June 30. www.reuters.com/world/americas/canada-rescinds-digital-services-tax-bid-advance-trade-talks-with-us-2025-06-30/.

Ndonji, Margaret. 2021. "The Future Implications of the Proposed Data Protection Regulations, 2021 on Conduct of Elections and Subsequent Election Petitions in Kenya." Mitullah Shako & Associates, May 24. https://mitullahshakolaw.com/?s=Future+implications.

Nsour, Mohammad. 2003. "Fundamental Facets of the United States-Jordan Free Trade Agreement: E-Commerce, Dispute Resolution, and Beyond." *Fordham International Law Journal* 27 (2): 742–84. https://ir.lawnet.fordham.edu/ilj/vol27/iss2/9.

Office of the USTR. 2008. "2008 Trade Policy Agenda and 2007 Annual Report." https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/archives/2008/2008-trade-policy-agenda-and-2007-annua.

———. 2012. "Comment from Robert Hollyman, Business Software Alliance." January 13. www.regulations.gov/comment/USTR-2011-0020-0056.

———. 2015. "The Trans-Pacific Partnership: Ensuring a Free & Open Internet." Fact sheet. https://ustr.gov/sites/default/files/TPP-Ensuring-a-Free-and-Open-Internet-Fact-Sheet.pdf.

———. 2025. "USTR Releases 2025 National Trade Estimate Report." Press release, March 31. https://ustr.gov/about/policy-offices/press-office/press-releases/2025/march/ustr-releases-2025-national-trade-estimate-report.

OPC. 2019a. "Archived — Consultation on transborder dataflows." www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-transborder-dataflows/.

———. 2019b. "Commissioner concludes consultation on transfers for processing." Announcement, September 23. www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190923/.

Pollet, Mathieu and Pieter Haeck. 2025. "EU could postpone flagship ai rules, tech chief says." POLITICO, June 6. www.politico.eu/article/eu-could-postpone-parts-of-ai-rulebook-tech-chief-says/.

Rachovitsa, Adamantia and Niclas Johann. 2022. "The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch *SyRI* Case." *Human Rights Law Review* 22 (2): ngac010. https://doi.org/10.1093/hrlr/ngac010.

Rangel, Daniel. 2022. "WTO General Exceptions: Trade Law's Faulty Ivory Tower." Public Citizen, February 4. www.citizen.org/article/wto-general-exceptions-trade-laws-faulty-ivory-tower/.

Renshaw, Jarrett. 2025. "Exclusive: US pushes countries for best offers by Wednesday as tariff deadline looms." Reuters, June 3. www.reuters.com/business/us-pushes-countries-best-offers-by-wednesday-tariff-deadline-looms-2025-06-02/.

Resnikoff, Jason. 2023. "How Bill Clinton Became a Neoliberal." *Jacobin*, August 31. https://jacobin.com/2023/08/a-fabulous-failure-review-bill-clinton-neoliberalism-capitalism.

Roberts, Dan and Ryan Felton. 2016. "Trump and Clinton's free trade retreat: a pivotal moment for the world's economic future." *The Guardian*, August 20. www.theguardian.com/us-news/2016/aug/20/trump-clinton-free-trade-policies-tpp.

Ryan, Michael Patrick. 1998. *Knowledge Diplomacy: Global Competition and the Politics of Intellectual Property*. Camden, UK: Bloomsbury Academic.

Samuelson, Pamela and Hal R. Varian. 2002. "The 'New Economy' and Information Technology Policy." In *American Economic Policy in the 1990s*, edited by Jeffrey A. Frankel and Peter R. Orszag, chapter 6. Cambridge, MA: The MIT Press. https://lawcat.berkeley.edu/record/1118039/files/infopolicy.pdf.

Scassa, Teresa. 2018. "The USMCA locks Canada in on digital trade — and at a worrying time." *Maclean's*, October 4. https://macleans.ca/facebook-instant-articles/the-usmca-locks-canada-in-on-digital-trade-and-at-a-worrying-time/.

Scott, Robert E. 2003. "The high price of 'free' trade: NAFTA's failure has cost the United States Jobs across the nation." Briefing Paper 147, November 17. Washington, DC: Economic Policy Institute. www.epi.org/publication/briefingpapers_bp147/.

Serra, Narcís and Joseph E. Stiglitz, editors. 2008. *The Washington Consensus Reconsidered: Towards a New Global Governance*. Oxford, UK: Oxford University Press.

Stiglitz, Joseph E. and Adam S. Hersh. 2015. "The Trans-Pacific Free-Trade Charade." Project Syndicate, October 2. https://www.project-syndicate.org/commentary/trans-pacific-partnership-charade-by-joseph-e--stiglitz-and-adam-s--hersh-2015-10.

Stupp, Catherine. 2016. "European Commission paralysed over data flows in TiSA trade deal." *Euractiv*, October 11. www.euractiv.com/section/trade-society/news/european-commission-paralysed-over-data-flows-in-tisa-trade-deal/.

The App Association. 2019. "The Office of the Privacy Commissioner of Canada's 'Consultation on Transfers for Processing — Reframed Discussion Document." Comment, August 6. https://actonline.org/wp-content/uploads/080619-ACT-Comments-re-Canada-OPC-Data-Transfers-Reframed.pdf.

The White House. 1997. "The Framework for Global Electronic Commerce." July 1. https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html.

———. 2000. "United States and Jordan Sign Historic Free Trade Agreement." Briefing Room, October 24. https://clintonwhitehouse5.archives.gov/WH/new/html/Tue_Oct_24_163554_2000.html.

———. 2021. "Executive Order on Promoting Competition in the American Economy." Presidential Actions, July 9. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/.

———. 2025a. "America First Trade Policy." Presidential Actions, January 20. www.whitehouse.gov/presidential-actions/2025/01/america-first-trade-policy/.

———. 2025b. "Regulating Imports with a Reciprocal Tariff to Rectify Trade Practices that Contribute to Large and Persistent Annual United States Goods Trade Deficits." Presidential Actions, April 2. www.whitehouse.gov/presidential-actions/2025/04/regulating-imports-with-a-reciprocal-tariff-to-rectify-trade-practices-that-contribute-to-large-and-persistent-annual-united-states-goods-trade-deficits/.

———. 2025c. "Report to the President on the America First Trade Policy Executive Summary." Fact Sheet, April 3. www.whitehouse.gov/fact-sheets/2025/04/report-to-the-president-on-the-america-first-trade-policy-executive-summary/.

Thompson, Kirsten. 2019. "Privacy Commissioner Proposes Consent be Required for Transborder Data Flows." *Dentons Data* (blog), April 27. www.dentonsdata.com/privacy-commissioner-proposes-consent-be-required-for-transborder-data-flows/.

Treisman, Rachel. 2025. "Trump's tariffs are so far-reaching they include several remote, uninhabited islands." NPR, April 3. www.npr.org/2025/04/03/nx-s1-5350897/trump-tariffs-heard-mcdonald-remote-islands.

Uematsu, Masafumi and Toru Tsunashima. 2020. "Divided internet — China and US switch places as data powerhouse." Nikkei Asia, November 26. https://vdata.nikkei.com/en/newsgraphics/splinternet/.

US Chamber of Commerce. 2023. "U.S. Chamber and Other Associations Letter to NSC/NEC on Digital Trade." November 7. www.uschamber.com/international/trade-agreements/u-s-chamber-and-other-associations-letter-to-nsc-nec-on-digital-trade.

Vaidhyanathan, Siva. 2016. "Was Obama Silicon Valley's President?" *The Nation*, December 13. www.thenation.com/article/archive/was-obama-silicon-valleys-president/.

Williams, Brock R. 2013. "Trans-Pacific Partnership (TPP) Countries: Comparative Trade and Economic Analysis." Congressional Research Service, July 7. www.congress.gov/crs-product/R42344.

Yuhas, Alan. 2016. "Congress will abandon Trans-Pacific Partnership deal, White House concedes." *The Guardian*, November 12. www.theguardian.com/business/2016/nov/12/tpp-trade-deal-congress-obama.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY: Hachette Book Group.

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