

Making NAFTA Worse

Giveaways for Big Tech in the USMCA

The United States-Mexico-Canada Agreement (USMCA) was signed in 2018 by President Trump to replace and modernize the older North American Free Trade Agreement (NAFTA). The agreement was notable for making progress on several issues, including strong and enforceable labor standards and largely removing controversial corporate tribunals that undermined sovereignty and democratic policymaking.

Pharmaceutical companies furiously opposed the USMCA after congressional Democrats successfully demanded the elimination of intellectual property terms that contribute to high medicine prices. However, a certain powerful industry was thrilled with the final deal, as Big Tech [secured](#) a host of extreme “digital trade” provisions, which many in Congress didn’t even realize were included until it was too late.

Multiple reports indicate how Big Tech lobbyists indulged in “[regulatory capture](#)” of the U.S. government’s trade policies. Through [cultivating personal relationships](#) and leveraging “[special relationships](#)” with those in power, Big Tech and its cronies were able to [create and institutionalize](#) a new set of purported digital trade rules. Borrowing from the playbook used previously by pharmaceutical and tobacco companies, Big Tech set out to preemptively kneecap any domestic attempts at regulating the growing tech sector.

Of particular interest to Big Tech companies were provisions that:

- Ensure the “[free flow of data across borders](#),” enabling data brokers and Big Tech companies to offshore American data despite clear risks to the privacy rights of American citizens and the offshoring of data-related jobs;
- Prohibit [source-code disclosure](#) as a condition to market access, thereby limiting the ability of Congress to establish rules regarding the transparency and accountability of AI systems;
- Implement “[safe harbor](#)” for intermediaries, despite increasing bipartisan consensus that online platforms must do more to check the spread of dangerous and illegal content;
- Sweeping so-called “[non-discrimination](#)” provisions could be used to [stymie regulations](#) aimed at ensuring a fairer and more competitive digital economy under the guise of [preventing discrimination](#).

Roll Call

'A real gift to Big Tech': Both parties object to immunity provision in USMCA

FINANCIAL TIMES

Why Silicon Valley wins big from the USMCA

POLITICO

Tech world's USMCA win

The Dallas Morning News

Big Tech's big win - Washington buckled in the USMCA

Each of these provisions is straight out of Big Tech's [digital trade wishlist](#), which seeks to [pre-empt](#) the ability of governments to introduce regulations that could affect their bottom lines or hold them accountable, irrespective of the consequent harm to public interest.

The USMCA was not the first time that Big Tech companies tried to include extreme digital trade provisions in a trade agreement. [The first such attempt, the Trans-Pacific Partnership Agreement \(TPP\)](#), was signed by President Obama in 2016. Trump railed against the TPP on the campaign trail and, once in office, withdrew the U.S. from the unpopular pact. Trump loved to hate the TPP, but that did not stop him from borrowing the deal's "digital trade" chapter and pasting it into the USMCA.

Interestingly, this cut-paste job, too, did not escape the interference of Big Tech lobbyists, who worked to whittle down the already limited exceptions and qualifiers included in the TPP. The USMCA, therefore, allows for [far fewer derogations](#) than the TPP, thereby further limiting the sovereign ability of signatories to regulate the



digital ecosystem. For instance, the TPP recognizes that parties may have their own regulatory regimes regarding cross-border data flows and the location of computing facilities. These provisions are not included in the USMCA.

The USMCA's July 2020 entry into force was a [big win](#) for the tech industry, as this was the first time that such extreme digital trade rules were codified in a binding and enforceable trade agreement that included the U.S. Following the USMCA, the first Trump administration also included similar provisions in an “executive-only” digital trade agreement with Japan, a pact that stirred controversy by circumventing Congress.

“The TPP rules (and its successor CPTPP) are carefully designed to constrain the ability of governments to regulate a rapidly changing digital environment in areas including consumer rights, privacy, other human rights issues, anti-competitive practices, labor law, government data, cyber security, and national security.”

- Burcu Kilic, [Digital trade rules: Big Tech's end run around domestic regulations](#), Heinrich Boll Stiftung, 2021

Following the signing of the USMCA, Big Tech sought to cement these provisions into international law in a patchwork of new trade agreements, including the [World Trade Organisation's Joint Statement Initiative on E-Commerce](#) (JSI) and the [Indo-Pacific Economic Framework for Prosperity](#) (IPEF).

However, responding to the rising awareness of the harms of these terms, the Biden administration wisely chose to [withdraw](#) U.S. support for these controversial provisions at the JSI and not to pursue those provisions in its IPEF negotiations, a move that brought [predictable outrage](#) from [Big Tech](#) and its lobbyists, while being lauded by many [members of Congress](#), [civil society groups](#) and [smaller tech companies](#).

The Biden administration [sought to pivot](#) American trade policy away from one that put the interests of big corporations over the interests of workers and consumers. By seeking to reorient trade policy away from the standard neoliberal playbook where big corporations make huge profits while the rest of society waits for wealth to trickle down, the Biden administration sought to end the longstanding pursuit of trade



policies that encouraged a global race to the bottom in terms of wages and labor standards, environmental impacts, and other socio-economic harms.

Digital Trade Under Trump 2.0: More Handouts to Big Tech?

Despite some [reports](#) of tension between nationalist and neoliberal groups in President Trump's inner circle, all signs indicate that the Trump administration favors the maximalist Big Tech agenda for digital trade.

Several [news reports](#) cover in excruciating [detail](#) how [titans](#) from Big Tech have been [lining](#) up to [pledge fealty](#) to President Trump. From Zuckerberg and Musk to Bezos and Pichai, this exercise of “kissing the ring” comes with an expectation that President Trump will place their interests at the forefront of his trade agenda.

Taken together with [previous reports](#) that indicate the historic proximity of the USTR to big business interests, this unedifying confluence of money and power will certainly work to upend the Biden administration's re-framing of trade policy to protect the interests of workers, consumers, and small industries.

Given President Trump's [faith](#) in [deregulation](#), as seen already in the case of the [AI industry](#), as well as his [distrust](#) of [Congress](#), it's likely that he will place little to no importance on ensuring that lawmakers have the ability to regulate the technology sector in the public interest, the primary reason for the USTR's change in position at the JSI.

The administration has already made its [intent clear](#) with [repeated warnings](#) to the European Union regarding the implementation of digital regulations aimed at protecting the privacy of European citizen's data, ensuring greater competition in the online market, and ensuring the safety of online platforms. President Trump's pick for USTR, Jamieson Greer, has also [made it clear](#) during his confirmation hearings that the U.S. will seek to push an “aggressive digital trade agenda.”

President Trump and others in his administration have also indicated that the U.S. will [retaliate against countries](#) that implement any public interest regulation of the technology ecosystem that could affect the bottom lines of American companies.

Allowing a deregulatory agenda to continue to be codified in the USMCA and other enforceable trade agreements would have disastrous effects on the regulation of the tech industry globally and, as a consequence, for the many millions of people and small businesses whose rights are directly impacted by a laissez-faire attitude to the regulation of the tech industry.



For instance, digital trade provisions mandating algorithmic secrecy are akin to enabling pharmaceutical companies to market drugs without pre-authorization from the Food and Drug Administration (FDA). Given the growing ubiquity of AI-based systems in policing and justice, insurance, housing, employment, healthcare provision, etc., ensuring that algorithms are not perpetuating or exacerbating biases will be vital to ensuring a fairer and more just society. In a similar vein, ensuring that data of American citizens cannot be exploited by tech companies is crucial to protecting the rights of vulnerable populations.

The Importance of Source Code Disclosure

“The ever-expanding use of software in products and services means that countries’ regulatory and judicial authorities face a growing number of situations where they need to determine whether the software is consistent with regulatory or legal requirements. Conclusive assessments may require the analysis of source code and, even where they could in principle be achieved through other means, may prove cheaper and easier to complete by accessing the source code.”

- Dorobantu, Ostmann and Hitrova, [Source code disclosures: A primer for trade negotiators](#), Alan Turing Institute, 2021

[Dorobantu, Ostmann, and Hitrova](#) point out that source code access can be useful in a number of situations. For example, software can be designed/used in ways that treat competitors unfairly. Notably, several Big Tech companies, including [Google](#) and [Amazon](#) have prioritized their own products and services over that of competitors when ranking search results. Ex-ante enforcement of competition law may require regulators to access source code of these platforms in order to ensure they function in a fair manner.

In equality-related laws, software is increasingly being used to make decisions such as [hiring/firing](#), determining credit or social benefits eligibility, predictive policing, etc. Ensuring that algorithms used in such products do not exacerbate racial, gender, and other biases can be essential to ensure that both the public and private sectors meet non-discrimination and other social obligations. A [number of states](#) already have laws in place that require an audit of algorithms used for purposes of employment. Modern AI laws, such as Europe’s AI Act, also provide significant transparency



requirements for high-risk AI systems, though they fall short of mandating full source code disclosure. Therefore, AI regulation implementing transparency mandates may [fall foul](#) of digital trade rules mandating source code secrecy.

In data protection, software can contain malicious code that intentionally or otherwise allows user data to be captured and shared with third parties. Ensuring that software does as it says may require access to source code. This may be particularly true of software embedded in consumer products, particularly those directed at children or vulnerable populations or those that may capture sensitive personal information.

In product safety and consumer protection: software can cause product safety violations in several areas, from transport to health via medical devices. Malicious or poorly written code can cost lives, particularly when used in devices that play a critical safety role. It may be important for such devices to undergo pre-emptive safety tests, which may need to include access to source code. Independent researchers and regulators may also need access to source code to gauge a host of unethical or illegal practices, for instance, the intentional degradation of battery life in smartphones.

For environmental protection, software and the algorithms used therein can be embedded within products used to regulate environmental impacts, such as emission controls in cars. Scrutiny of source code could have prevented the infamous case of [Volkswagen](#) enabling millions of cars with emissions-cheating software.

In right-to-repair regulation, a [number](#) of recent [laws attempt](#) to promote the [right to repair](#), that is, the ability for consumers to access the necessary hardware and software to repair their electronic devices themselves or through independent third parties. Access to source code could be essential in [promoting this right](#), given the growing integration of software that uses algorithms in all manner of consumer goods and other devices, from tractors to wheelchairs.

Why Restrictions on Cross-border Data Transfers?

Targeted [restrictions](#) on [cross-border data transfers](#) can be used to (a) protect civil liberties such as privacy, (b) ensure regulators and other government entities can access data to carry out their supervisory functions, and (c) for economic and strategic reasons.

When stored in foreign jurisdictions, American citizen's data is subject to foreign laws and privacy practices, which may not ensure appropriate standards of data security. Enforcement of privacy or related claims in foreign jurisdictions may also be difficult.



Offshoring of data also implies that jobs related to that data, such as in the AI supply chain, are denied to the U.S. workforce.

It is worth noting that the Biden administration issued [Executive Order 14117](#) in February 2024, directing the Department of Justice to implement [restrictions](#) on the bulk flow of American sensitive personal data to countries of concern. The Executive Order notes that “The growing exploitation of Americans’ sensitive personal data threatens the development of an international technology ecosystem that protects our security, privacy, and human rights.” Thereafter, President Biden signed into law the [Protecting Americans’ Data from Foreign Adversaries Act, 2024](#), which provides the [Federal Trade Commission](#) with the authority to take action against data transfers to certain countries.

Any attempt to implement similar regulations to restrict the transfer of personal data on rights-based grounds – that could help consumers, workers, and vulnerable groups protect their sensitive personal data and thereby seek to dismantle the surveillance-capitalism-based model of the Internet – could be challenged under the USMCA. State privacy and data protection regulations that restrict data transfers or the foreign processing of American data, such as biometrics, could also be threatened.

A recent [report](#) by Rethink Trade highlights the dangers of broad ‘free flow of data’ provisions to domestic data governance measures noting that “Each of these U.S. policies [referring to state and federal policies that restrict cross-border data storage] fundamentally conflicts with the notion that binding international rules should prohibit governments from the regulating cross-border data flows or data storage locations.”

In the fast-changing technology landscape, it is ill-advised to limit the ability to regulate cross-border data flows, particularly when [such measures](#) are increasingly being considered around the world to protect [private and public](#) interests.

Would Extreme Digital Trade Rules Help Innovation in the US?

Extreme digital trade rules in the USMCA could also be used to challenge a host of other regulations that aim to ensure greater competitiveness and fairness in the digital economy. For instance, provisions on [non-discrimination](#), investment, and financial services could be used to challenge laws that seek to limit the power of Big Tech to abuse their monopolies or avoid paying their fair share of taxes.

Big Tech has already been [pushing for the U.S. to take action](#) against digital competition laws in a number of jurisdictions ranging from Korea to the EU. Such attempts are only likely to increase and hinder efforts at creating a fairer digital



economy, where small companies can compete on a level playing field with Big Tech giants.

While some policymakers close to Big Tech companies may argue that formalizing a deregulatory agenda in trade negotiations would benefit the U.S. by providing its Big Tech companies more space to earn profits in the short run, in the long run, this will certainly backfire. Public safety and ethical concerns could lead to consumers and businesses across the world reducing their reliance on U.S.-developed tech in favor of more open or ethical models. For instance, note the importance given to public digital infrastructure-related technologies at the United Nations and G20 meetings over the last few years.

In addition, the continued monopolization by many U.S. companies in the global digital economy is only likely to lead to inefficiencies and slowly reduce the competitiveness of the U.S. tech sector. As demonstrated by the release of the Chinese Deepseek LLM, technological innovation is difficult to slow down or police on a global scale. In an ecosystem where technology development is being driven by companies from all parts of the world, the significant differentiator is likely to be the ethical and safety-related assurances that a particular technology can provide.

This makes it all the more important for the U.S. to ensure that it takes the lead in promoting robust and rights-based regulatory systems for technology. The signing of trade agreements that limit U.S. sovereignty and the ability to implement public interest regulation is likely a shortsighted move.

Removing Giveaways to Big Tech in the USMCA

The USMCA contains a clause that requires the parties to review the agreement in 2026, following which the agreement can be renewed as-is, modified, or allowed to expire in 2036. In an early executive order on trade, the Trump administration announced that it would conduct [public consultations](#) for the USMCA review.

Civil rights activists, [labor unions](#), and other public interest groups need to come together to oppose the continued inclusion of dangerous digital trade provisions in the USMCA. As seen with the signing of the USMCA in 2018 (adopted by the U.S. Congress in 2020), concerted pushback can limit the influence of big corporations over the trade negotiation process.

It was only due to the strong opposition of [Democrats in Congress](#), backed by labor unions and other progressive groups that strong labor and environmental provisions



were introduced, while damaging intellectual property rules that impede access to affordable medicines were removed from the [USMCA](#).

Changes Required in the USMCA

To protect the fundamental rights of U.S. citizens, workers, and marginalized communities and ensure Congress' sovereign right to regulate the digital ecosystem in the public interest, the USMCA must be amended to:

- Remove provisions that protect source code from disclosure to governments, regulators, and independent researchers or that restrict the right to repair.
- Remove provisions that confer 'safe harbor' on intermediaries
- Remove or retool provisions in the digital, investments, and services chapters that allow for anti-discrimination claims to be brought against laws that meet legitimate public interests, such as ensuring competition in the digital economy or taxation of large digital companies.
- Remove provisions that restrict the ability of governments to restrict cross-border transfers of data or require the establishment of local computing facilities.
- Avoid the inclusion of new-age digital trade provisions that restrict the ability of governments to regulate the AI ecosystem, regulate the use of encryption, and proselytize the use of digital identities.

