Before the United States Trade Representative

Docket Number USTR-2025-0004

"Operation of the Agreement between the United States of America, the United Mexican States, and Canada"

Written Comments from Rethink Trade

November 3, 2025

Rethink Trade thanks the United States Trade Representative (USTR) for the opportunity to submit comments with regard to the operation of the United States-Mexico-Canada Agreement (USMCA).

Rethink Trade is a program of the American Economic Liberties Project (AELP). AELP, a non-profit research and advocacy organization, is a thought leader in the anti-monopoly movement and promotes policy changes to address today's crisis of concentrated economic power. The Rethink Trade program of AELP was established to intensify analysis and advocacy regarding the myriad ways that today's trade agreements and policies must be altered to undo decades of corporate capture and to deliver on broad national interests. This includes resilient supply chains and fair markets, creation and support of good jobs with workers empowered to earn decent wages, the public health and safety delivered by strong consumer and environmental protections, and the ability for those who will live with the results to decide the policies affecting their lives.

These comments focus in detail on three areas: USMCA outcomes measured with respect to trade flows and balance; improvements needed to USMCA digital trade rules to avoid international preemption threats especially in light of data security, right to repair, and other policies enacted by the U.S. federal and state governments since 2020; and USMCA labor rights and enforcement provisions needed for the Rapid Response Mechanism (RRM) to deliver on its promises. We also address Rules of Origin and wages. However, Rethink Trade urges USTR to use the mandatory USMCA six-year review also to renegotiate and improve other aspects of the pact. We convey our views on these additional matters as signatories to comments submitted by the Citizens Trade Campaign and Trade Justice Education Fund that describe the full range of improvements we seek, including to the environment, rules of origin, intellectual property, agriculture, investment, and other terms and as signatories to comments submitted by Health GAP and Public Citizen on changes to USMCA intellectual property rules needed to bolster access to affordable medicine.

During his first term, President Trump initiated a renegotiation of the North American Free Trade Agreement (NAFTA). He called NAFTA the worst trade deal ever and promised to end it, winning broad support among working-class Americans in the 2016 election.[1] As predicted by macroeconomic theory, decades of large, chronic global trade deficits have both deindustrialized the United States and fueled socioeconomic inequality. The hollowing out of former U.S. industrial centers[2] has contributed to adverse economic outcomes and a growing gap in life expectancy between Americans with and without college degrees.[3]

Trump signed a NAFTA 2.0 deal in 2018. Congressional Democrats would not enact it given concerns about insufficient protections for workers' rights and the environment, gaps in enforcement and new monopoly powers for pharmaceutical firms to raise medicine prices. Trump then renegotiated the NAFTA 2.0.[4] That deal, which he named the United States-Mexico-Canada Agreement (USMCA), came into force in 2020.

The approval of USMCA by wide bipartisan margins in Congress reflected that the pact was an improvement on NAFTA. However, at the time of the vote, many congressional Democrats, unions, and civil society groups remained skeptical about whether the USMCA could stop or even greatly diminish NAFTA's ongoing damage of race-to-the-bottom job offshoring by firms eager to exploit Mexico's low wages and lax environmental enforcement. Some were also concerned about new terms included in USMCA relative to NAFTA that threatened new harms. These terms included new constraints on signatory nations' regulation of digital platforms and new limits on food safety and other public interest safeguards. Concerns also included many problematic provisions from the original NAFTA, such as those that provided pharmaceutical firms monopoly rights to raise medicine prices that extend beyond the already troubling such rules established in the World Trade Organization. Thus, in supporting the USMCA, many noted that while USMCA was an improvement on NAFTA and the terms in the USMCA established a new floor that every future U.S. trade pact must meet, it did not represent a model going forward.

In contrast, Trump called the USMCA "the most important trade deal we've ever made by far" and promised it would be "the most modern, up-to-date, and balanced trade agreement in the

---

[1] Maggie Severns, "Trump Pins NAFTA, 'Worst Trade Deal Ever,' on Clinton," *POLITICO*, September 26, 2016, https://www.politico.com/story/2016/09/trump-clinton-come-out-swinging-over-nafta-228712; "An Examination of the 2016 Electorate, Based on Validated Voters," Pew Research Center, August 9, 2018, https://www.pewresearch.org/politics/2018/08/09/an-examination-of-the-2016-electorate-based-on-validated-voters/.

[2] David Autor, David Dorn, and Gordon Hanson, "The China Trade Shock: Studying the Impact of China's Rise on Workers, Firms, and Markets," accessed October 29, 2025, https://chinashock.info/.

[3] Josh Bivens, "Adding Insult to Injury: How Bad Policy Decisions Have Amplified Globalization's Costs for American Workers," Economic Policy Institute, July 11, 2017, https://www.epi.org/publication/adding-insult-to-injury-how-bad-policy-decisions-have-amplified-globalizations-costs-for-american-workers/; Anne Marie D. Lee, "Most Americans Can't Afford a $1,000 Emergency Expense, Report Finds," *CBS News*, January 23, 2025, https://www.cbsnews.com/news/saving-money-emergency-expenses-2025/; Anne Case and Angus Deaton, "Accounting for the Widening Mortality Gap Between American Adults With and Without a BA," Brookings, September 27, 2023, https://www.brookings.edu/articles/accounting-for-the-widening-mortality-gap-between-american-adults-with-and-without-a-ba/.

[4] Jacob Pramuk, "House Democrats and the White House Have a Deal to Move Forward with USMCA Trade Agreement," *CNBC*, December 10, 2019, https://www.cnbc.com/2019/12/10/house-democrats-and-trump-administration-reach-usmca-trade-deal.html.

history of our country."[5] He claimed the agreement would create 600,000 new American jobs[6] and a minimum of 80,000 new auto manufacturing jobs.[7] He declared USMCA was a monumental win for American farmers and ranchers that would boost American agricultural exports to Mexico and Canada by $2.2 billion.[8]

Trump's promises have not materialized in the USMCA's first five years of operation. Indeed, under USMCA, the U.S. goods trade deficit with Mexico grew 30 percent from $196.5 billion in 2019 to $253.7 billion in 2024 (adjusted for inflation);[9] with services factored in, the U.S. trade deficit with Mexico was a record $175.9 billion in 2024.[10] Manufacturing wages in Mexico remain about 40 percent lower than in China, and the offshoring of manufacturing facilities and jobs from the United States to Mexico continues. Trade Adjustment Assistance (TAA) petition data is only available for the first two years of the USMCA's operation because Congress has failed to reauthorize or fund the program that has otherwise been in operation since the Kennedy presidency. From July 1, 2020, to July 1, 2022, 249 certified TAA petitions cited Canada and/or Mexico for trade-related job losses with 41,357 U.S. workers affected.

With the USMCA's results not meeting Trump's promises, Trump committed to renegotiate the USMCA on the campaign trail in 2024.[11]

The 2026 review of the USMCA presents an opportunity to reshape U.S. trade policy starting with the United States' largest trading partners and closest neighbors. Rethink Trade urges the

---

[5] Donald Trump, "Remarks by President Trump on the United States-Mexico-Canada Agreement," White House Archives, October 1, 2018, https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-united-states-mexico-canada-agreement/.

[6] The White House, "President Donald J. Trump's United States-Mexico-Canada Agreement Delivers a Historic Win for American Workers," White House Archives, January 29, 2020, https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trumps-united-states-mexico-canada-agreement-delivers-historic-win-american-workers/.

[7] Donald Trump, "Remarks by President Trump at a USMCA Celebration with American Workers | Warren, MI," White House Archives, January 30, 2020, https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-usmca-celebration-american-workers-warren-mi/; Donald Trump, "Remarks by President Trump at the Economic Club of New York | New York, NY," White House Archives, November 12, 2019, https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-economic-club-new-york-new-york-ny/.

[8] The White House, "President Donald J. Trump's United States-Mexico-Canada Agreement Delivers a Historic Win for American Workers."

[9] Calculated using "Domestic Exports" and "Imports for Consumption," U.S. International Trade Commission DataWeb, accessed October 28, 2025, https://dataweb.usitc.gov/; adjusted for inflation using "Consumer Price Index for All Urban Consumers," Federal Reserve Bank of St. Louis, accessed October 28, 2025, https://fred.stlouisfed.org/series/CPIAUCSL.

[10] "U.S. Trade in Goods and Services by Selected Countries and Areas, 1999–Present," U.S. Bureau of Economic Analysis, accessed October 28, 2025, https://www.bea.gov/data/intl-trade-investment/international-trade-goods-and-services; adjusted for inflation using "Consumer Price Index for All Urban Consumers," Federal Reserve Bank of St. Louis, accessed October 28, 2025, https://fred.stlouisfed.org/series/CPIAUCSL.

[11] Donald Trump, "Donald Trump Addresses the Detroit Economic Club," *Roll Call*, October 10, 2024, https://rollcall.com/factbase/trump/transcript/donald-trump-speech-detroit-economic-club-october-10-2024/. Improving the balance of North American trade can help deliver on Trump's broader promises to end the U.S. trade imbalance, create U.S. industrial jobs, and rebuild U.S. manufacturing. To date, the data show outcomes trending away from these goals. In 2024, the U.S. goods trade deficit was over $1.2 trillion; with services factored in, the trade deficit was a record $918.4 billion. See, e.g., Ana Swanson, "U.S. Trade Deficit Hit Record in 2024 as Imports Surged," *The New York Times*, February 5, 2025, https://www.nytimes.com/2025/02/05/business/economy/us-trade-deficit-2024-record.html.

Trump administration to use the mandatory six-year review included in the USMCA as an opportunity to renegotiate the agreement and secure terms that can better deliver on more balanced trade, wage gains and U.S. manufacturing capacity, and job creation that President Trump promised for USMCA while removing those that conflict with U.S. law or undermine public interests. Such changes would ensure that the USMCA is more favorable to U.S. workers, farms, small businesses, and consumers. These comments describe specific improvements needed to RRM and significant changes needed to the digital trade chapter majorly altered to deliver trade wins to U.S. constituencies beyond just the largest U.S. corporations.

1. USMCA "Digital Trade" Provisions that Conflict with U.S. Federal or State Policies Must be Eliminated and Those Limiting Future Domestic Policies with Broad Support Must be Modified

Since 2022, Rethink Trade has conducted extensive analysis of the conflicts presented by the USMCA Digital Trade chapter with domestic technology regulation efforts at the state and federal levels. The existing digital trade chapter preempts and conflicts with U.S. technology policy enacted at the federal and state level since USMCA's 2020 effective date as well as congressional proposals with broad bipartisan support. As USTR Greer has stated repeatedly, U.S. digital policy must be made at home. Changes to existing USMCA digital trade terms are required to avoid the USMCA imposing a form of international preemption against laws *enacted* by Congress and state legislatures. The existing USMCA terms also conflict with scores of additional laws with broad bipartisan support proposed in Congress and in state legislatures.

In its last two sessions alone, Congress has introduced several bipartisan bills that would be deemed illegal "trade barriers" by USMCA Digital Trade chapter terms. These bills include the Artificial Intelligence Risk Evaluation Act of 2025,[12] the Facial Recognition Act of 2025,[13] the Protecting Americans' Data from Foreign Adversaries Act of 2024 (which passed the

[12] U.S. Senate, Artificial Intelligence Risk Evaluation Act of 2025, S 2938, 119th Congress, 1st sess., introduced in Senate September 29, 2025, https://www.congress.gov/bill/119th-congress/senate-bill/2938/. This bill is sponsored by Sens. Josh Hawley (R-MO) and Richard Blumenthal (D-CT). Bill language could conflict with Digital Trade chapter terms on source code secrecy, specifically the following provision: "Each covered advanced artificial intelligence system developer shall (…) provide to the Secretary, on request, materials and information (…) which may include (…) (A) the underlying code of the advanced artificial intelligence system."

[13] U.S. House, Facial Recognition Act of 2025, 119th Congress, 1st sess., introduced in House July 23, 2025, https://www.congress.gov/bill/119th-congress/house-bill/4695/. Bill language could conflict with Digital Trade chapter terms on source code secrecy, specifically the following provision: "No investigative or law enforcement officers may begin using a new facial recognition system or information derived from it unless that system is first submitted to independent testing."

Republican-controlled House unanimously and was enacted into law in 2024),[14] and the Justice in Forensic Algorithms Act of 2024.[15]

As the nation's leading consumer, tech and union organizations have also noted in a joint letter,[16] these specific USMCA "digital trade" provisions must be altered or eliminated during the review:

Alter Data Flows and Storage Rules to Accommodate Data Security and Privacy Laws: The 2018 USMCA Cross-Border Transfer of Information by Electronic Means and Location of Computing Facilities terms (USMCA Articles 19.11 and 19.12, respectively) conflict with U.S. laws and regulations enacted since USMCA's 2020 effective date as the United States has joined other nations in regulating data flows and storage for security and privacy reasons.[17] These USMCA provisions broadly forbid regulation of where data may be sent and stored. The ban on data flow limits does not apply only between the United States and other signatory countries but obligates nations to allow data flow to China and other third countries, directly undermining U.S. policy requiring the opposite. And the "public policy" exception to the ban on data flow regulation is designed to be useless. It replicates the necessity and chapeau tests of the deeply flawed World Trade Organization (WTO) General Exceptions. Nations' efforts to satisfy the language used in the USMCA digital public policy exception have failed in 46 of 48 attempts to use similar language at WTO since the WTO's 1995 start.[18] There is no exception to the storage provision.

During the USMCA six-year review, these digital trade data provisions must be rewritten to eliminate the current USMCA ban on regulation of data flows and storage so as to accommodate new U.S. laws enacted since USMCA's 2020 effective date, such as the 2024

---

[14] U.S. House, Protecting Americans' Data from Foreign Adversaries Act of 2024, HR 7520, 118th Congress, 2nd sess., introduced in House March 5, 2024, https://www.congress.gov/bill/118th-congress/house-bill/7520/. This bill was sponsored by three House Republicans and three House Democrats. Bill language could conflict with Digital Trade chapter terms on data flows and storage, specifically the following provision: "It shall be unlawful for a data broker to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive data of a United States individual to—(1) any foreign adversary country; or (2) any entity that is controlled by a foreign adversary." The bill was included as Division I in a national security package signed by President Biden in April 2024: U.S. House, Making Emergency Supplemental Appropriations for the Fiscal Year Ending September 30, 2024, and for Other Purposes, HR 815, 118th Congress, 1st sess., introduced in House February 2, 2023, https://www.congress.gov/bill/118th-congress/house-bill/815/.

[15] U.S. House, Justice in Forensic Algorithms Act of 2024, HR 7394, 118th Congress, 2nd sess., introduced in House February 15, 2024, https://www.congress.gov/bill/118th-congress/house-bill/7394/. Bill language could conflict with Digital Trade chapter terms on source code secrecy, specifically the following provision: "Any results or reports resulting from analysis by computational forensic software shall be provided to the defendant, and the defendant shall be accorded access to both an executable copy of and the source code for the version of the computational forensic software."

[16] "Letter: End Big Tech 'Digital Trade' Rules in USMCA, Unions, Consumer, Digital Rights Groups Tell USTR Greer," AFL-CIO, American Economic Liberties Project, Center for Digital Democracy, Consumer Federation of America, Demand Progress Education Fund, Economic Security Project, NETWORK Lobby for Catholic Social Justice, Rethink Trade, Tech Oversight Project, Trade Justice Education Fund, and United Steelworkers, July 9, 2025, https://rethinktrade.org/letters-filings/digital-trade-usmca/.

[17] See report annexed to these comments: Daniel Rangel, Jai Vipra, and Lori Wallach, "The Digital Trade Data Heist: Trade Agreement Limits on Data Transfer and Storage Regulation Could Undercut Data Governance," Rethink Trade, February 2025, https://rethinktrade.org/digitaltradeheist/.

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

Protecting Americans' Data from Foreign Adversaries Act. Passed unanimously in the GOP-controlled House and signed into law in April 2024, it forbids data brokers from selling Americans' personal data to offshore entities subject to the jurisdiction of adversarial nations to protect American national security and individual privacy.[19] Absent modification, these rules also will conflict with the 2025 "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" regulation, which forbids the transfer of "bulk sensitive personal data or United States Government-related data" to a foreign country of concern, or by a national of such a country.[20] The 2018 USMCA data flow and storage terms must be modified so as to eliminate direct conflict with state laws,[21] including Montana's 2023 Genetic Information Privacy Act, which bans storage of genetic/biometric data collected in Montana in countries sanctioned in any way by the U.S. federal government.[22] It is not in the U.S. national interest to preserve trade-pact terms that conflict with our own laws.

We described the ways in which other countries around the world avoid such conflicts in our recent report, "The Digital Trade Data Heist: Trade Agreement Limits on Data Transfer and Storage Regulation Could Undercut Data Governance," which is annexed to these comments.[23] These approaches offer models for alternative language. We also have developed language that accommodates data security and privacy goals we would be pleased to share on request.

Eliminate Special Source Code Secrecy Rule: The Source Code provision (USMCA Article 19.16) provides special secrecy protections to source code and also extends to algorithms. It forbids governments from requiring government or public access to algorithmic information and code, even when necessary to repair our own cars, tractors, phones, and other property or ensure child online safety, fair competition, or other national interests. Among the laws that this provision could undermine is Texas's 2023 Securing Children Online Through Parental Empowerment (SCOPE) Act, which requires digital service providers to disclose algorithmic information to third-party researchers, with an exemption for small businesses. There also are at least eight U.S. states that have enacted right-to-repair laws covering farm equipment, cars, motorized wheelchairs, and more with 50+ such state laws pending, which is why business, consumer, farm, and other organizations that prioritize Right to Repair have also submitted

---

[19] U.S. House, Protecting Americans' Data from Foreign Adversaries Act of 2024, HR 7520, 118th Congress, 2nd sess., introduced in House March 5, 2024, https://www.congress.gov/bill/118th-congress/house-bill/7520/. The bill was included as Division I in a national security package signed by President Biden in April 2024: U.S. House, Making Emergency Supplemental Appropriations for the Fiscal Year Ending September 30, 2024, and for Other Purposes, HR 815, 118th Congress, 1st sess., introduced in House February 2, 2023, https://www.congress.gov/bill/118th-congress/house-bill/815/.

[20] Federal Register, *Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, A Rule by the Justice Department*, January 8, 2025, https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-accessto-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern.

[21] "Big Tech's 'Digital Trade' Agenda Threatens States' Tech Policy Goals," Rethink Trade, last updated September 17, 2024, https://rethinktrade.org/big-techs-digital-trade-agenda-threats-states-tech-policy-goals/.

[22] Montana Code § 30-23-104, Genetic Information Privacy Act, last amended 2023, https://archive.legmt.gov/bills/mca/title_0300/chapter_0230/part_0010/section_0040/0300-0230-0010-0040.html.

[23] Rangel, Vipra, and Wallach, "The Digital Trade Data Heist: Trade Agreement Limits on Data Transfer and Storage Regulation Could Undercut Data Governance."

comments to this docket we have also joined that raise this problem.[24] The USMCA Source Code rule makes the key right-to-repair obligations to share digital keys, diagnostic tests, and the like illegal trade barriers. As well, antitrust enforcement, like that initiated in the first Trump term against Big Tech, often requires disclosure of source code and detailed algorithmic information to discover self-preferencing and other anti-competitive practices or requires disgorgement of some proprietary code in settlements.

The exception is limited to source code disclosure orders or requests made by regulatory or judicial bodies "for a specific investigation, inspection, examination, enforcement action, or judicial proceeding" with disclosure limited to the regulatory body. The exception to this provision does not cover the sorts of policies noted above or pre-screening of artificial intelligence (AI) in sensitive sectors, which some bills propose. Many AI safety regulations require that the developers or users of AI technologies provide information about those systems to regulators as a condition of their sale or use. Senators Josh Hawley and Richard Blumenthal introduced the Artificial Intelligence Risk Evaluation Act of 2025, which requires that the developers of advanced AI systems provide information to the Secretary of Energy upon request, which may include the underlying code of and data used to train the AI systems. Developers are required to participate in this program in order to be able to deploy AI tools, meaning that this is an ex ante control not covered by the exception in USMCA Article 19.16.2. Other regulations require that AI systems used for specific purposes (like law enforcement) be subject to independent testing or share algorithmic information with criminal defendants if automated decision technologies are used in determining case outcomes. Affected bills include the Facial Recognition Act of 2025 and the Justice in Forensic Algorithms Act of 2024 introduced in Congress, as well as Idaho's law on pretrial risk assessment tools, which has been in effect since 2019.[25]

There is no need for this Source Code rule, and it must be eliminated during the USMCA six-year review. Indeed, few nations' pacts include such a term. The WTO Agreement on Trade-Related Aspects of International Property Rights (TRIPS) Article 10 already requires: "Computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention." Thus, software developers have global copyright protection against others copying specific code formulations that underpin software. And TRIPS Article 39 on "Protection of Undisclosed Information" requires all WTO nations to protect business-confidential information. This obligation applies to all kinds of business-confidential information, including proprietary code and algorithms, as long as such information is secret, has commercial value because it is secret, and has been subject to reasonable steps to be kept secret. Thus, if a country requires the disclosure of firms' code and/or algorithmic information and then passes it on to competitors, it would violate TRIPS Article 39.

Alter Non-Discrimination Provision to Accommodate Anti-Monopoly Policies: The USMCA language in the Non-Discriminatory Treatment of Digital Products provision (USMCA Article 19.4) twists the traditional trade non-discrimination concept and language found in past pacts to

[24] American Economic Liberties Project is a signatory of a comment to this docket alongside other organizations in the Repair Coalition regarding the impacts of the Digital Trade chapter on the right to repair. See that submission for further detail on USMCA implications for the right to repair and necessary fixes.
[25] Idaho Code § 19-1910, Pretrial Risk Assessment Tools, last amended 2019, https://legislature.idaho.gov/statutesrules/idstat/title19/t19ch19/sect19-1910/.

ensnare policies that do not differentiate based on national origin but that may have a disproportionate effect on dominant services and products. Past U.S. FTA E-Commerce chapters with digital product non-discrimination rules differentiated between de jure and de facto discrimination. Policies that actually treat domestic and foreign products, owners, or developers differently were simply forbidden. But if a facially neutral policy happened to have a disproportionate effect on some foreign firms or products, a showing of discriminatory intent was required to find a violation. In contrast, the USMCA provision makes any policies affecting not just digital products, but also digital platforms, that have a greater effect on a foreign entity an illegal trade barrier, even if they apply to domestic and foreign firms equally. This guts competition policy, which necessarily targets dominant firms and that, in the digital sphere, will hit U.S. firms not because they are American but because they are large.

Smaller, innovative American tech firms rely on digital competition policies in Korea, Japan, and other nations to gain market access and create new products and American jobs. These laws in other countries are replicated in U.S. bipartisan proposals like the Open App Markets Act;[26] the U.S. Journalism Competition and Preservation Act, introduced in the last congressional session by 11 Democratic and 10 Republican senators to push dominant platforms to negotiate payment for news content they use;[27] and the American Innovation and Choice Online Act, which prohibits covered platforms from self-preferencing their own products via their platforms.[28] The digital products non-discrimination language used in pre-USMCA U.S. trade-pact E-Commerce chapters, such as in KORUS, is a fine starting point for an approach that does not label most competition policies illegal trade barriers. However, WTO rulings on intent require tweaks to clarify the previous language. We have developed language that accommodates data security and privacy goals we would be pleased to share on request.

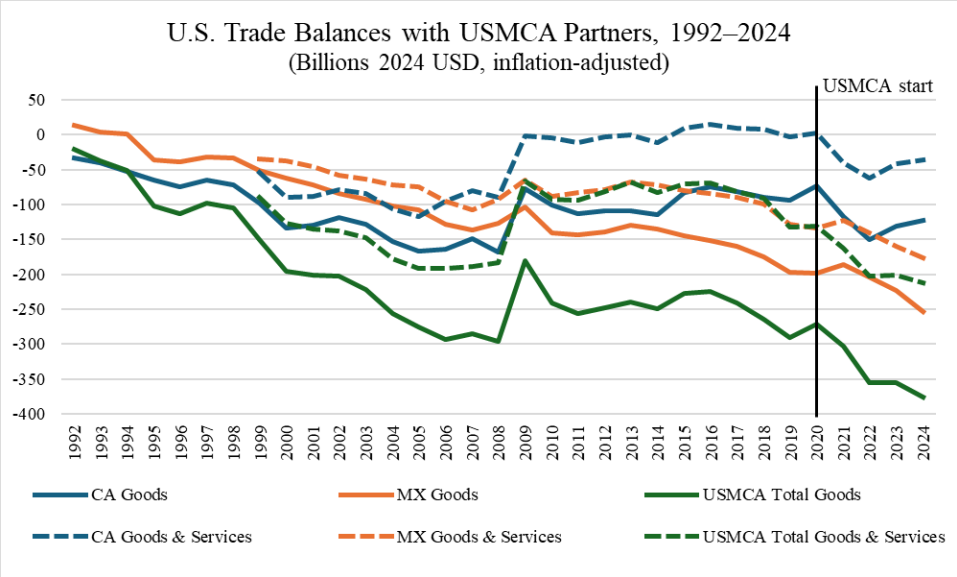
Eliminate the Provision Locking In and Exporting to Mexico and Canada the Section 230 Liability Waiver: USMCA's Interactive Computer Services rule (USMCA Article 19.17) requires USMCA signatory countries to enact a Section 230-style liability waiver for platforms regarding the content that they carry. **President Trump as well as former President Biden and many in Congress support at least changes to Section 230, if not its revocation. This provision must be eliminated during the USMCA six-year review.**

2. USMCA Has Not Delivered Balanced Regional Trade as the U.S. Trade Deficit with Mexico Deepened Significantly Since 2020

The United States has had a bilateral goods trade deficit with Mexico each year since 1995,[29] the year after NAFTA went into effect, and a bilateral goods trade deficit with Canada each year

[26] U.S. Senate, Open App Markets Act, S 2153, 119th Congress, 1st sess., introduced in Senate June 24, 2025, https://www.congress.gov/bill/119th-congress/senate-bill/2153.
[27] U.S. Senate, Journalism Competition and Preservation Act of 2023, 118th Congress, 1st sess., introduced in Senate March 30, 2023, https://www.congress.gov/bill/118th-congress/senate-bill/1094.
[28] U.S. Senate, American Innovation and Choice Online Act, 117th Congress, 1st sess., introduced in Senate October 18, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/2992.
[29] "Trade in Goods with Mexico," U.S. Census Bureau, accessed October 29, 2025, https://www.census.gov/foreign-trade/balance/c2010.html.

since at least 1985.[30] In his 2018 Rose Garden remarks on the USMCA, Trump lamented "trade deficits totaling more than $2 trillion" with Canada and Mexico since the start of NAFTA.[31] But contrary to Trump's promises, the USMCA did not reverse the trend of ever-expanding U.S. trade deficits.



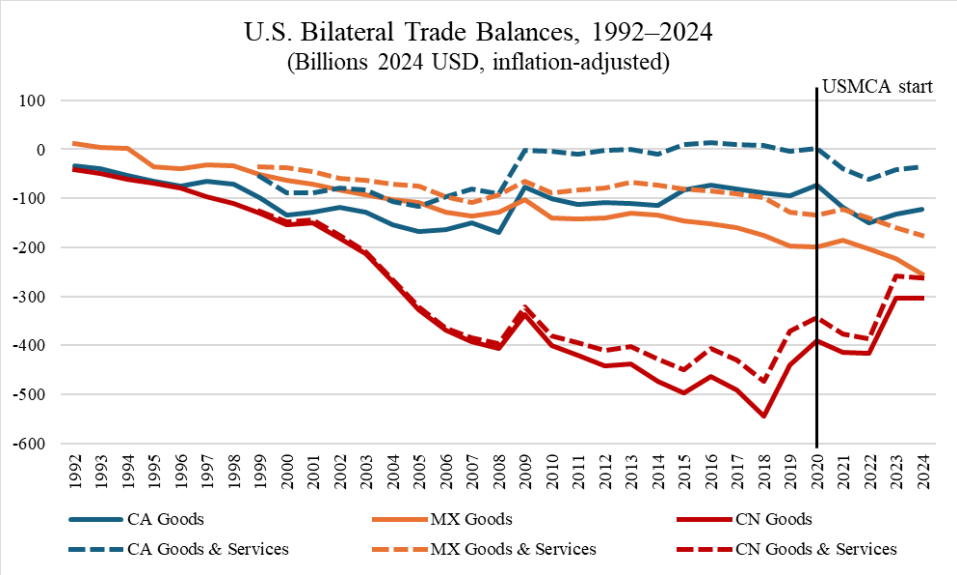
Goods trade balances calculated using Domestic Exports and Imports for Consumption data from U.S. International Trade Commission DataWeb. Goods and services balances from Bureau of Economic Analysis. Adjusted for inflation using St. Louis Fed CPI. Accessed October 28, 2025.

With the USMCA having so far failed to raise Mexican wages significantly such that manufacturing wages there remain lower than in China, Mexico—as well as comparably low-wage Vietnam—became offshore producers' favorite new venue for production destined for the U.S. market after Trump imposed tariffs on goods from China in his first term.

Notably, from 2020 to 2024, the U.S. goods trade deficit with its USMCA partners increased by $104 billion. In the same period, the U.S. bilateral trade deficit with China *decreased* by $86 billion:

[30] "Trade in Good with Canada, U.S. Census Bureau, accessed October 29, 2025, https://www.census.gov/foreign-trade/balance/c1220.html

[31] Donald Trump, "Remarks by President Trump on the United States-Mexico-Canada Agreement," White House Archives, October 1, 2018, https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-united-states-mexico-canada-agreement/.



Goods trade balances calculated using Domestic Exports and Imports for Consumption data from U.S. International Trade Commission DataWeb. Goods and services balances from Bureau of Economic Analysis. Adjusted for inflation using St. Louis Fed CPI. Accessed October 28, 2025.

On the one hand, this shift in trade flows lowers U.S. dependency on Chinese imports. It may reflect a growing trend in "nearshoring" with companies seeking low-wage manufacturing venues trying to derisk their China exposure and avoid U.S. tariffs on Chinese goods. However, that imports into the United States from Mexico—as well as from Vietnam—have surged as Chinese imports declined reflects a core ongoing problem: Mexico's wages remain extremely low and indeed are only slightly higher than Vietnam's and 40 percent lower than those in China. As discussed below, addressing the wage gap must be a key outcome of the review.

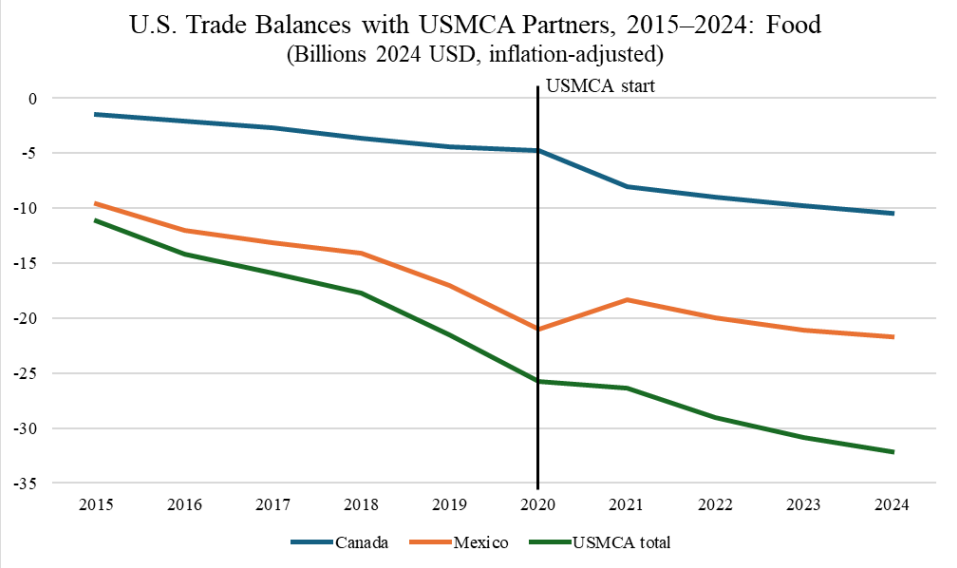
Moreover, as noted below, the USMCA's rules of origin (although better than those of NAFTA in many regards) still allow duty-free imports into the United States of goods with significant Chinese and other third-country content. For instance, according to one recent study, about a quarter of Mexican exports' value was Chinese content.[32]

Another growing concern is increasing investment by Chinese companies in Mexico to use USMCA as an export platform to evade tariffs on Chinese goods.[33] The Baker Institute published a working paper in January 2025 which found over 200 Chinese investments in Mexico worth

[32] Enrique Dussel Peters, "21.2 Por Ciento, el Valor Agregado Chino de las Exportaciones Mexicanas a Estados Unidos" ("21.2 Percent, the Chinese Added Value of Mexican Exports to the United States"), *La Jornada*, October 9, 2024, https://www.jornada.com.mx/2024/10/09/opinion/018a1eco.
[33] Christine Murray, Nassos Stylianou, Irene de la Torre Arenas, and Dan Clark, "How China is Setting Up Shop in Mexico," *Financial Times*, December 16, 2024, https://ig.ft.com/china-mexico-tariffs/.

billions of dollars.[34] A September 2025 Brookings study found evidence for illegal transshipment of Chinese products via Mexico in power transformers, iron and steel, and auto parts.[35]

Notably, the USMCA agricultural trade balance did not fare better. The first Trump administration claimed that the USMCA would deliver major wins for U.S. farmers and ranchers, including significant increases in exports.[36] But the U.S. food trade deficit with Mexico and Canada during USMCA grew more than $6 billion from 2020 to 2024 as import growth outpaced exports.



Domestic Exports and Imports for Consumption data from U.S. International Trade Commission DataWeb. Adjusted for inflation using St. Louis Fed CPI. Accessed October 1, 2025. Food HTS codes include HTS Chapters 1 through 22 less select non-food products, including live animals not primarily used for meat or other products; inedible animal or plant products; horticultural products; vegetable plaiting materials; industrial acids; and animal feed.

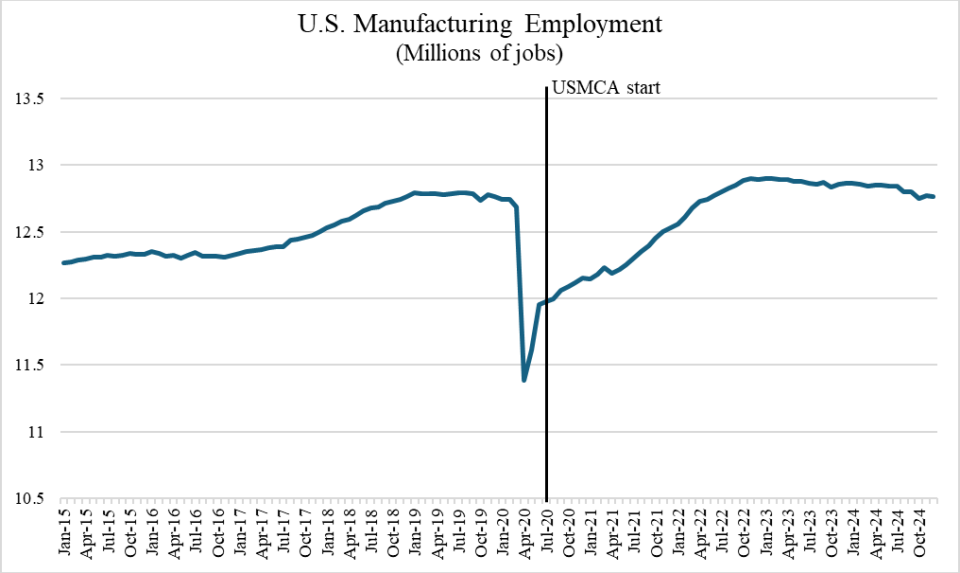
It is worth also noting that U.S. manufacturing employment has not significantly increased per Trump's promises. In fact, according to the U.S. Bureau of Labor Statistics, there were the same amount of manufacturing jobs (12.76 million) in December 2019 as in December 2024:

---

[34] Gabriel Collins, Tony Payan, and David A. Gantz, "Quantifying Investments in Mexico by China-Linked Entities," Baker Institute for Public Policy, January 30, 2025, https://www.bakerinstitute.org/research/quantifying-investments-mexico-china-linked-entities.

[35] Joshua P. Meltzer and Maricarmen Barron Esper, "Is China Circumventing US Tariffs Via Mexico and Canada?," Brookings, September 23, 2025, https://www.brookings.edu/articles/is-china-circumventing-us-tariffs-via-mexico-and-canada/.

[36] Donald Trump, "Remarks by President Trump at a Signing Ceremony for the United States-Mexico-Canada Trade Agreement," White House Archives, January 29, 2020, https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-signing-ceremony-united-states-mexico-canada-trade-agreement/.



Data from U.S. Bureau of Labor Statistics. Accessed October 17, 2025.

As the outcome data show, if President Trump is committed to rebalancing U.S. trade and to creating a North American manufacturing powerhouse to increase resilience and counter unfair trade practices from other countries—with the United States playing a significant role in making things along with its partners—then clearly, the USMCA review and renegotiation must secure better labor rights enforcement, direct measures to raise wages in Mexico, and tighten USMCA rules of origin to minimize third-country content entering the U.S. market duty-free via USMCA. As well, the United States (or, even better, the three USMCA countries) must raise their Most Favored Nation tariff rates on key manufactured goods and aspects of their supply chains so that paying inconsequential tariffs for access into the U.S. market for goods made in Mexico without complying with USMCA rules is no longer a viable strategy.

3. The USMCA's Rapid Response Mechanism Has Shown that Labor Enforcement Can Deliver Gains for Workers, but Key Improvements Are Required to Level the Playing Field and End the Race to the Bottom

The USMCA includes stronger labor standards compared to previous agreements and a novel new system intended to address the race to the bottom in wages and work conditions that the original NAFTA generated. This innovative legal tool, called the Rapid Response Mechanism (RRM), complements the state-to-state dispute settlement mechanisms of older trade agreements. The USMCA also included specific commitments by Mexico to overhaul its labor relations system to establish independent federal and state labor courts, conciliation centers to help resolve labor disputes, and democratic union practices—including personal, direct, secret-ballot voting to approve collective bargaining agreements and elect union leadership. The 2019 reform has begun to transform labor relations in Mexico and allowed the RRM to emerge as a useful tool for independent unions.

Yet despite five years of the RRM's operation, the implementation of Mexico's historic labor reform, and several increases in the federal minimum wage, wages in Mexico remain suppressed. Employer-aligned unions continue to represent many workplaces and are deeply entrenched. The fewer independent unions have made only limited progress in narrowing the wage gap with the United States for the relatively small share of workers they represent. Thus, **the USMCA review must deliver necessary changes to the stronger Rapid Response Mechanism so that it can help to reverse decades of trade-related job losses and strengthen labor standards across North America.**

In September 2025, Rethink Trade published a first-of-its-kind comprehensive analysis of RRM cases decided under the USMCA.[37] In dozens of RRM cases during the first five years of its operation, tens of thousands of workers have made real gains, including reinstatements after retaliatory firings, new opportunities for independent unions to organize, and stronger contracts.

In its first five years, the RRM has produced important results. It led to reinstatement of workers fired for union activity, expanded access to trainings on freedom of association, and supported new opportunities for independent unions. Between July 2020 and June 2025, the United States initiated 37 RRM cases targeting 36 facilities involving mining, call centers and air transport services, food, electronics, apparel, and, most notably, automotive sector manufacturing. Tens of thousands of workers in facilities where RRM cases succeeded have made real gains. But the USMCA has not delivered on topline promises to end the race to the bottom in wages and labor conditions or balance regional trade. Wages in Mexico remain very low despite some gains. Workers in the automotive and electronics manufacturing sectors still earn only $3 to $5 per hour, even as productivity approaches U.S. levels. Manufacturing wages in Mexico remain about 40 percent lower than in China.

Key findings from this research include:

A. The governments are "resolving" too many cases without securing long-term gains for workers.

By mid-2025, of 32 concluded cases initiated by the U.S. government concerning labor violations in Mexico, half were deemed "resolved during review," eight resulted in a formal Course of Remediation, and six advanced to panels. The USMCA text does not clearly outline the consequences of cases being "resolved during review." The increasing tendency to close cases without a Course of Remediation or panel action calls into question whether this approach genuinely tackles union-busting practices or holds companies accountable through a clear record of denial-of-rights violations.

B. Remediation has been real, but it is often standardized and insufficient in some cases.

Common remedies agreed by governments to end cases without panel activation include neutrality statements, worker reinstatements, and freedom of association (FOA) trainings. These measures are important steps, particularly the reinstatement of workers fired for their union activities or preferences. However, commitments to grant union access to facilities or recognize and bargain with petitioner unions have been less frequent. Strengthening remedies to prioritize

[37] See report annexed to these comments: Daniel Rangel and Lori Wallach, "Closing the Gap: Evaluating Rapid Response Labor Mechanism Outcomes and Charting a Path Through the 2026 USMCA Review," Rethink Trade, September 2025, https://rethinktrade.org/closingthegaprrm/.

actions that enable independent unions to organize and bargain collectively would help advance the core objectives of the RRM.

C. Progress has been made on freedom of association, but there is less movement on collective bargaining.

Twelve workplaces out of 32 concluded RRM cases saw workers gain new union representation and/or contracts, but a larger share of RRM cases did not produce such results. Early RRM cases were notably successful in delivering durable gains for workers. Later cases suggest that corporations have developed strategies to persuade authorities that limited actions amount to sufficient remediation without enabling workers to organize independent unions or negotiate strong collective bargaining agreements. The fact that half of all concluded RRM cases have not resulted in new union representation and/or a new or revised contract raises questions about the effectiveness of the mechanism to fulfill its ultimate objectives.

D. Secrecy about why petitions are rejected or even how many are filed chills use of the RRM and hinders accountability.

There is no public information on the total number of petitions filed under the RRM, nor any transparency about the reasons some were rejected. Through a FOIA request, we discovered that 56 petitions were filed during the first five years of the RRM, although one was later withdrawn. The U.S. government initiated action on 38 cases: 36 resulting from petitions and two self-initiated. But there is limited public information about why 19 petitions were rejected or otherwise did not trigger activation of the mechanism. The lack of transparency that has marked the RRM's initial years is a key area requiring improvement.

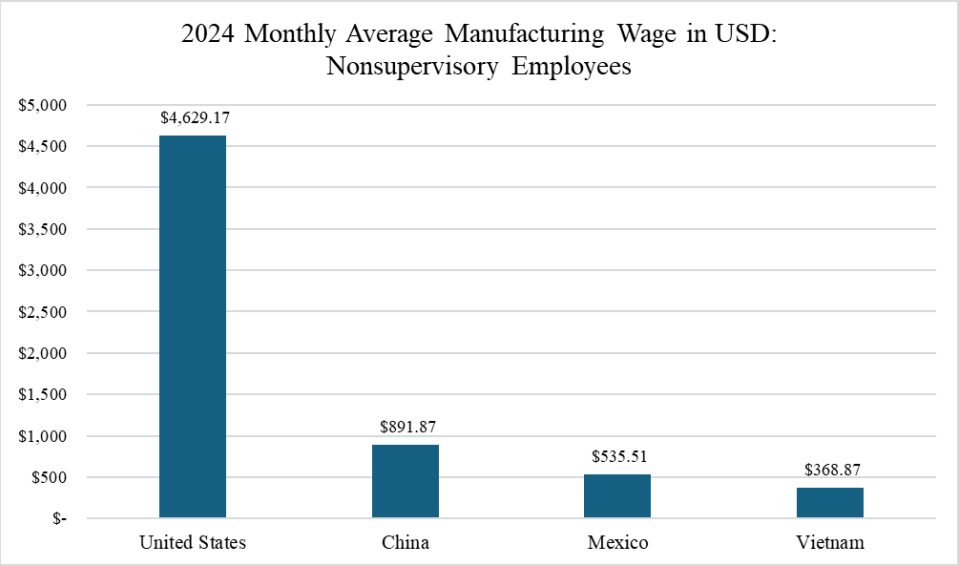
In an October 2025 report, the Independent Mexico Labor Export Board (IMLEB) found that Mexico is not in compliance with its labor obligations under the USMCA.[38] IMLEB was established by the USMCA implementing legislation to monitor Mexico's commitment to its Federal Labor Law. The IMLEB report specifically mentions issues with obligations under the RRM: It found that, even in cases where the United States and Mexico both call for sanctions for labor law violations, these sanctions have not been imposed. IMLEB found that Mexico has made progress in union representation and wage increases, but protection of workers' rights is lacking, including protecting workers from violence and other retaliation when they exercise the right to associate.

Mexican manufacturing wages remain 40 percent lower than Chinese manufacturing wages in an equivalent sector and 88 percent lower than U.S. manufacturing wages. Wages have not increased substantially despite the RRM's operation, the implementation of Mexico's historic labor reform, and several increases in the Mexican federal minimum wage. In 2024, unionized Mexican workers experienced their highest wage gain in two decades, yet real wages rose by just 2.2 percent year-over-year, highlighting the slow pace of meaningful improvement.[39]

---

[38] Independent Mexico Labor Expert Board, Report, October 6, 2025, https://aflcio.org/sites/default/files/2025-10/IMLEB_REPORT_2025_10_06.pdf.

[39] Gerardo Hernández, "Salarios Contractuales Alcanzaron en 2024 el Crecimiento Real Más Alto en Dos Décadas," *El Economista*, January 15, 2025, https://www.eleconomista.com.mx/capital-humano/2024-salarios-contractuales-alcanzaron-crecimiento-real-alto-dos-decadas-20250115-742129.html.



Authors' elaboration based on official government data. See annexed Rethink Trade report "Closing the Gap: Evaluating Rapid Response Labor Mechanism Outcomes and Charting a Path Through the 2026 USMCA Review" for more detail.

The persistent wage gap between manufacturing wages in the United States and Mexico is arguably the main driver of the U.S. government having certified over one million jobs lost due to NAFTA under the Trade Adjustment Assistance (TAA) program. The congressional authorization for TAA was allowed to lapse on July 1, 2022, meaning the Department of Labor can no longer accept petitions or provide training or income support for trade-affected workers who seek it. This, along with the petition filing requirements and possible lack of widespread knowledge of TAA benefits, make it impossible to know how many U.S. workers have lose their jobs due to USMCA-related factors.

However, TAA petition data is available for the first two years of the USMCA's operation. From July 1, 2020, to July 1, 2022, there were 251 petitions filed which cited Canada and/or Mexico. 249 of these petitions were certified as trade-related job losses, including 41,357 affected workers.[40] This means that the wage gap and persistent labor rights enforcement shortcomings in Mexico have continued to encourage job offshoring.

According to recent data from Economic Commission for Latin America and the Caribbean, foreign direct investment (FDI) from the United States in Mexico's manufacturing sector grew by 23 percent in 2024.[41] The manufacturing industry was the leading recipient of foreign investment in Mexico, accounting for 53 percent of the total in 2024.

U.S. manufacturing facilities have continued relocating to Mexico under USMCA. For instance, in 2024, John Deere announced plans to move a manufacturing facility from Iowa to Mexico by

[40] Petition data from "Trade Adjustment Assistance for Workers," U.S. Department of Labor, accessed October 17, 2025, https://www.dol.gov/agencies/eta/tradeact/data.
[41] Pamela Cruz, "Mexico Breaks Foreign Direct Investment Record: $45.3 Billion in 2024, Highest Annual Total Since 2013," Mexican Press Agency, July 22, 2025, https://mexicanpressagency.org/newsroom-posts/foreign-direct-investment/.

the end of 2026.[42] Volvo Group, which makes Volvo and Mack semi-trucks, announced a new $700 million truck factory in Mexico in 2024 while laying off up to 1,000 workers in Pennsylvania, Virginia, and Maryland plants.[43] As well, major U.S. companies are standing up new production in Mexico to make vehicles for sale in the United States that many expected to be located here. In 2021, GM announced over $1 billion in investment for Mexican electric vehicle production.[44] Tesla committed to building its next factory in Mexico in 2023.[45] GE Aerospace this year announced $550 million to expand aircraft engine manufacturing facilities in Mexico.[46] Major U.S. retailers including Walmart and Amazon have expanded their sourcing and logistics operations in Mexico in recent years.[47]

In order to end the race to the bottom in wages and working standards across North America, the RRM system must be strengthened. In addition to USMCA reforms aimed at directly raising North American wages, details of which we understand have been included in labor union submissions, Rethink Trade recommends a set of targeted adjustments and systemic improvements to the RRM. While detailed information is provided in Rethink Trade's recent report,[48] in sum:

Targeted Adjustments:

1. **Shorten the respondent Party's period for internal review.** The respondent Party's 45-day internal review period should be shortened to 30 days, matching the complainant Party's timeline. While the U.S. government has demonstrated that such investigations can be completed within this shorter timeframe, Mexico's greater access to facilities and investigative tools makes a longer period unnecessary. More importantly, the current 45-day window often results in cases being superficially "resolved during review," with companies offering quick fixes that fail to address deeper violations of workers' rights. A

---

[42] Matt Ott, "Struggling with Falling Demand for Farm Equipment, Deere & Co. Announces Nearly 600 Layoffs," *The Associated Press*, July 1, 2024, https://apnews.com/article/john-deere-layoffs-agriculture-jobs-c7db7e8ed24cd2ecaf8343be3dec82d9.

[43] "Volvo Picks Monterrey for $700 Mln Mexico Truck Plant," *Reuters*, August 23, 2024, https://www.reuters.com/business/autos-transportation/volvo-picks-monterrey-700-mln-mexico-truck-plant-2024-08-23/; Jack Roberts and Deborah Lockridge, "Mack, Volvo Trucks Laying Off as Many as 1,000," *Heavy Duty Trucking*, April 28, 2025, https://www.truckinginfo.com/10239576/mack-trucks-announces-layoffs.

[44] Michael Wayland, "GM to Invest $1 Billion in Mexico for Electric Vehicle Production, Angering UAW Members," *CNBC*, April 29, 2021, https://www.cnbc.com/2021/04/29/gm-to-invest-1-billion-in-mexico-for-electric-vehicle-production.html.

[45] Chris Isidore, "Tesla to Build Next Plant in Mexico," *CNN*, March 1, 2023, https://www.cnn.com/2023/03/01/business/tesla-mexico-plant/index.html.

[46] Teresa De Alba, "GE Aerospace to Invest MX$550 Million in Mexico Expansion in 2025," *Mexico Business News*, September 22, 2025, https://mexicobusiness.news/aerospace/news/ge-aerospace-invest-mx550-million-mexico-expansion-2025.

[47] Peter S. Goodman, "'OK, Mexico, Save Me': After China, This Is Where Globalization May Lead," *The New York Times*, January 1, 2023, https://www.nytimes.com/2023/01/01/business/mexico-china-us-trade.html; "Amazon, Mercado Libre, Geodis Announce US$1.2 Billion Investment," *Mexico Business News*, September 16, 2025, https://mexicobusiness.news/trade-and-investment/news/amazon-mercado-libre-geodis-announce-us12-billion-investment.

[48] See report annexed to these comments: Daniel Rangel and Lori Wallach, "Closing the Gap: Evaluating Rapid Response Labor Mechanism Outcomes and Charting a Path Through the 2026 USMCA Review," Rethink Trade, September 2025, https://rethinktrade.org/closingthegaprrm/.

30-day limit would push for more substantive evaluations and reduce incentives for shallow remediation.

2. **Extend or modify the Interagency Labor Committee's deadline to determine whether to invoke a panel.** Congress should extend or modify the 60-day deadline imposed on the Interagency Labor Committee to decide whether to request a panel after invoking the RRM. Under current rules, the U.S. government has only 15 days following Mexico's 45-day internal review to make this determination, which can lead to premature closure of cases based on short-term or superficial remedies. Extending the deadline by 15 to 45 days—or allowing extensions when necessary—would provide sufficient time to assess whether commitments are being effectively implemented and ensure decisions reflect lasting improvements in workers' rights.
3. **Require Parties to consult with stakeholders—especially petitioners—when developing remediation actions, and disclose investigation findings while safeguarding witness workers.** Including petitioners in the Course of Remediation process would help ensure that remedies address ongoing violations, while sharing investigation outcomes in writing would strengthen accountability and improve the RRM's effectiveness.
4. **Clarify that a "Resolved During Review" outcome counts as a Denial of Rights Determination.** The mechanism is designed around escalating penalties, making it critical that corporations involved in violations face lasting consequences and an increased risk of future cases. The growing trend of categorizing outcomes as "resolved during review" raises concerns that governments and companies may use this designation to avoid a formal "first strike." Explicitly stating in the USMCA text that such cases qualify as Denial of Rights Determinations would strengthen deterrence and preserve the integrity of the penalty system established in Article 31-A.10.
5. **Clarify that administrative and judicial authorities' actions can constitute a Denial of Rights under the RRM.** The agreement does not require attributing violations solely to companies or governments, which is critical since employers often rely on protection unions or local authorities to obstruct workers' organizing and bargaining efforts. However, in practice, there has been reluctance to address violations involving administrative or judicial misconduct through the RRM. To reaffirm the Parties' intent, the USMCA text should be clarified to explicitly include such actions within the scope of the mechanism.

Systemic Improvements:

1. **Add a substantive obligation requiring all USMCA Parties to ensure employers bargain in good faith.** While the RRM has been effective in addressing freedom of association violations, remediation related to collective bargaining has been rare, in part because Mexican labor law does not explicitly require employers to negotiate in good faith. The result is that domestic enforcement often focuses on compliance with strike procedures rather than employers' bargaining conduct. To strengthen workers' ability to secure union contracts, the USMCA should include a clear obligation for all Parties to impose a duty to bargain in good faith, with a commitment for Mexico to amend its Federal Labor Law accordingly.
2. **Require Mexico's Federal Center for Labor Conciliation and Registration to have sanctioning authority.** While the RRM has advanced labor rights enforcement, it cannot

address all violations. Amending the USMCA to require that Mexican law grant the Federal Center sanctioning authority— an initiative already approved by the lower house of Congress but stalled in the Senate—would bolster enforcement and extend protections nationwide.

3. **Isolate fact-finding aspects of the RRM process and make it equally applicable to all USMCA Parties.** Currently, governments must both investigate petitions and—in the case of Mexico—defend companies accused of labor rights violations, a conflict that undermines credibility. The process also lacks transparency, with neither petitioners nor companies having access to investigators' reports or evidence the other party submits. Establishing an independent body—potentially modeled on precedents like the U.S.–Cambodia Textile Agreement or the Bangladesh Accord—would enhance impartiality, ensure stakeholders receive findings, and build trust in the system. Finally, extending the RRM to cover facilities in the United States and Canada would guarantee equal protection for workers across all Parties and prevent distortions in labor standards and competition.

However, even if the RRM is improved during the six-year review, it would take decades for case-by-case labor rights enforcement action to build up sufficient density of independent unions to bring Mexican wages to a level where workers there can purchase the goods they are now making almost exclusively for export, which would cut the incentives to offshore U.S. production to Mexico.

That is why it is critical that the USMCA's Rules of Origin (ROO) are tightened and wage levels are directly addressed.

4. Rules of Origin Must Be Tightened and Wage Levels Directly Addressed

Strong rules of origin are not only critical to ensuring that the beneficiaries of a trade deal are the countries that signed it, but also to ensure labor and environmental standards benefit people in the countries in the deal. Low rules of origin mean parts made by exploiting workers or the environment could be imported and put into goods assembled in one of the countries instead of creating high-standard supply chains.[49]

The USMCA raised the ROOs for some sectors, like autos and auto parts and some steel products, relative to NAFTA. Auto trade is 18 percent of U.S. goods trade under the USMCA. However, the U.S. Most Favored Nation (MFN) tariff for passenger vehicles of 2.5 percent is so low that some automakers manufacturing in Mexico for the U.S. market opt to pay the tariffs to evade compliance with the USMCA's stronger rules of origin that would limit Chinese and other third-country supply chain inputs.

[49] We expect that the UAW submission to this docket will include more a detailed analysis on USMCA Rules of Origin and Labor Value Content. We associate ourselves with the UAW submission.

President Biden used Section 232 to implement a melted and poured rule for steel from Mexico,[50] which may help explain the positive U.S. trade balance in those goods because steel largely made elsewhere but finished in Mexico could no longer gain duty-free access through USMCA. But for many goods, the inputs and parts making up the majority of the value of a finished good can come from China and other countries yet still get duty-free access into the United States if assembled in Mexico or Canada.

Mexico now has a sizeable trade deficit with China[51] and has shifted into having a chronic global trade deficit, even as it has a large bilateral trade surplus with the United States in part because the duty-free export platform it provides into the United States draws input imports into Mexico for use in Mexican assembly factories. **During the USMCA six-year review, the Regional Value Content rule must be raised for many more sectors beyond autos as well as further increases in the auto sector to drive investment in North American supply chain manufacturing.**

The USMCA also included a novel ROO—called the Labor Value Content (LVC)—for the auto sector. It requires that a percentage of a car's overall value and the value of certain parts be made by workers making at least $16 per hour to qualify for USMCA duty-free access. It was discussed popularly as a way to try to raise wages in Mexico and also ensure some of the sector's supply chain manufacturing and assembly occurred in the United States and Canada.

But the program was designed largely to target only foreign automakers, not the U.S. "Big Three," and the types of workers (including some professional salaried workers) who could count in the average meant the $16 standard would not require higher line-worker salaries in Mexico. The LVC did nothing to raise wages in the auto sector in Mexico. Rather, it really was designed to force Japanese, Korea, European, and other automakers to start investing in the United States rather than only in Mexico for cars made to sell in the North American market under duty-free USMCA terms. But it did not work well for that goal either: First, the extremely low 2.5 percent U.S. MFN tariff rates for passenger cars meant some makers simply paid the tariffs rather than adjust how they operated. As well, the U.S. regulations issued to enact the LVC allowed automakers to self-certify that they met the rules, with no U.S. Department of Labor or other agenda research or verification into wage levels in specific Mexican, U.S., or Canadian plants to be able verify the $16-per-hour average was met.

Whether it was by design or problematic implementation, the LVC ROO has not raised wages in Mexico. That is a critical goal for a revised USMCA. **Independent unions in all three countries are calling for minimum wages by sector across countries as a way to immediately address the race to the bottom in wages and to avoid evasion through technical implementation maneuvers for other approaches.[52] For this approach to be**

---

[50] The White House, "A Proclamation on Adjusting Imports of Steel Into the United States," White House Archives, July 10, 2024, https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/07/10/a-proclamation-on-adjusting-imports-of-steel-into-the-united-states-7/.

[51] Roberto Morales, "México Dobla Déficit Comercial con China en 10 Años," *El Economista*, July 15, 2025, https://www.eleconomista.com.mx/empresas/mexico-dobla-deficit-comercial-china-10-anos-20250715-768204.html.

[52] Jared Laureles and Alexia Villaseñor, "Liga Sindical Propone Salario Mínimo Regional en Sectores Cubiertos por el T-MEC" ("Trade Union League Proposes Regional Minimum Wage in Sectors Covered by the USMCA"), *La Jornada*, October 30, 2025, https://www.jornada.com.mx/noticia/2025/10/30/sociedad/sindicatos-proponen-que-revision-al-salario-minimo-regional-se-incluya-en-el-tmec; María del Pilar Martínez, "Sindicatos Independientes

effective, at a minimum, the United States must raise its MFN tariff rates in covered sectors so that producers realize they must comply with USMCA wage, labor, and environmental rules and strong ROO if they want to benefit from duty-free USMCA access into the U.S. market. Ideally, the three USMCA countries would coordinate on such MFN tariff increases, creating a high-standard North American manufacturing zone.

Conclusion

Rethink Trade urges USTR to use the mandatory USMCA six-year review to renegotiate and improve aspects of the pact that significantly impact the U.S. trade balance, efforts to regulate tech and protect data privacy, and outcomes for workers across North America.

Changes to existing USMCA digital trade terms are required to avoid the USMCA imposing a form of international preemption against laws enacted by Congress and state legislatures. The existing USMCA terms also conflict with scores of additional laws with broad bipartisan support proposed in Congress and in state legislatures. Digital trade provisions on Cross-Border Transfer of Information by Electronic Means, Location of Computing Facilities, Source Code, Non-Discriminatory Treatment of Digital Products, and Interactive Computer Services must be altered or eliminated during the review. These changes are necessary to eliminate the current USMCA ban on regulation of data flows and storage so as to accommodate new U.S. laws enacted since USMCA's 2020 effective date; eliminate unnecessary source code secrecy rules standing in the way of the right to repair; accommodate anti-monopoly policies; and allow widely supported changes to or revocation of Section 230-style liability waivers for digital platforms.

The first five years of the USMCA have failed to rebalance U.S. trade. If President Trump is committed to rebalancing U.S. trade and to creating a North American manufacturing powerhouse to increase resilience and counter unfair trade practices from other countries—with the United States playing a significant role in making things along with its partners—then the USMCA review and renegotiation must secure better labor rights enforcement, direct measures to raise wages in Mexico, and tighten USMCA rules of origin to minimize third-country content entering the U.S. market duty-free via USMCA. As well, the United States (or, even better, the three USMCA countries) must raise their Most Favored Nation tariff rates on key manufactured goods and aspects of their supply chains so that paying inconsequential tariffs for access into the U.S. market for goods made in Mexico without complying with USMCA rules is no longer a viable strategy.

The USMCA review must deliver necessary changes to the stronger Rapid Response Mechanism so that it can help to reverse decades of trade-related job losses and strengthen labor standards across North America. In order to end the race to the bottom in wages and working standards across North America, the RRM system must be strengthened. In addition to USMCA reforms aimed at directly raising North American wages, Rethink Trade recommends a set of targeted

---

Impulsan Salario Mínimo Regional y Fortalecimiento del Capítulo Laboral del T-MEC" ("Independent Unions Promote Regional Minimum Wage and Strengthening of the USMCA Labor Chapter"), *El Economista*, October 15, 2025; see Jason Wade's remarks in "Press Release: First Comprehensive Review of USMCA Labor Cases Shows Tool Delivered Wins, but Structural Gaps Threaten Long-Term Success," Rethink Trade, September 25, 2025, https://rethinktrade.org/press-releases/usmcarrmreport/.

adjustments and systemic improvements to the RRM as listed in the third section of this submission.

During the USMCA six-year review, the Regional Value Content rule must be raised for many more sectors beyond autos as well as further increases in the auto sector to drive investment in North American supply chain manufacturing. Independent unions in all three countries are calling for minimum wages by sector across countries as a way to immediately address the race to the bottom in wages and to avoid evasion through technical implementation maneuvers for other approaches. For this approach to be effective, at a minimum, the United States must raise its MFN tariff rates in covered sectors so that producers realize they must comply with USMCA wage, labor, and environmental rules and strong ROO if they want to benefit from duty-free USMCA access into the U.S. market. Ideally, the three USMCA countries would coordinate on such MFN tariff increases, creating a high-standard North American manufacturing zone.

Annexes

The following reports provide more detail on the problems we summarize with the existing USMCA terms and the improvements that we urge USTR to undertake in the six-year review.

1. *Report:* Daniel Rangel, Jai Vipra, and Lori Wallach, "The Digital Trade Data Heist: Trade Agreement Limits on Data Transfer and Storage Regulation Could Undercut Data Governance," Rethink Trade, February 2025, https://rethinktrade.org/digitaltradeheist/.
2. *Report:* Daniel Rangel and Lori Wallach, "Closing the Gap: Evaluating Rapid Response Labor Mechanism Outcomes and Charting a Path Through the 2026 USMCA Review," Rethink Trade, September 2025, https://rethinktrade.org/closingthegaprrm/.
3. *Report:* Daniel Rangel and Lori Wallach, "International Preemption by 'Trade' Agreement: Big Tech's Ploy to Undermine Privacy, AI Accountability, and Anti-Monopoly Policies," Rethink Trade, March 2023, https://rethinktrade.org/reports/international-preemption-by-trade-agreement/.
4. *Report:* "Undermining AI Regulation in the U.S. and Abroad: The 'Digital Trade' Secrecy Ploy," Rethink Trade, July 2023, https://rethinktrade.org/reports/ai-report/.
5. *Report:* Daniel Rangel, Taylor Buck, Erik Peinert, and Lori Wallach, "'Digital Trade' Doublespeak: Big Tech's Hijack of Trade Lingo to Attack Anti-Monopoly and Competition Policies," Rethink Trade, November 2022, https://rethinktrade.org/reports/digital-trade-doublespeak-big-techs-hijack-of-trade-lingo-to-attack-anti-monopoly-and-competition-policies/.
6. *Report:* Anthony D. Rosborough, "Source Code: A Trade-Related Barrier to the Right to Repair," Transatlantic Consumer Dialogue, October 17, 2025.

rethink TRADE

AMERICAN ECONOMIC LIBERTIES PROJECT

The Digital Trade Data Heist: Trade Agreement Limits on Data Transfer and Storage Regulation Could Undercut Data Governance

Daniel Rangel
Jai Vipra
Lori Wallach

February 2025

DIGITAL TRADE BRIEFING PAPERS SERIES

RETHINK TRADE

rethinktrade.org

CONTENTS

EXECUTIVE SUMMARY

Around the world, governments are discussing and adopting policies that regulate the ways in which data is collected, transferred, and stored, with the goal of meeting myriad public interest objectives. The regulatory drive began with the vast majority of countries adopting personal data protection regimes, most of which impose limits on the cross-border movement of data. To date, 162 countries have passed national personal data–protection laws, and 75% of all countries have adopted some limits and conditions on the cross-border transfer of data. More recently, the United States and other countries have focused on data security, including related to important geopolitical interests. Lawmakers and regulators are deploying national security measures that restrict or outright prohibit certain transactions involving sensitive data. Moreover, experts and advocates are exploring ways to adequately tax the data economy, which could be deemed as effectively curbing certain international data transfers. The explosion of AI systems — trained on massive amounts of data — has raised questions about how to ensure that smaller companies have access to this critical resource, rather than it being monopolized by incumbent tech giants. These concerns have given momentum to data-sharing mandates and related policies.

Expansive rules in international trade agreements that impose binding restrictions on governments' abilities to regulate cross-border data flows and where data is stored run counter to these data governance efforts. For the past decade, certain tech interests have advocated for trade agreements to include strong limits on governments' abilities to regulate international data transfers and data location. These terms — often included in "digital trade" or "e-commerce" chapters or agreements — usually ban government regulation of international data transfers (cross-border data flows rules) and/or where data may be stored (location of computing facilities rules). Industry interests seek to lump all such polices together under what they consider the pejorative label of "data localization."

In the U.S., Congress, state legislatures, the military, NASA, and the White House have all enacted policies recently that would be undermined by rules banning data transfer and storage regulation. These include:

» ***Protecting Americans' Data from Foreign Adversaries Act of 2024:*** In March 2024, the U.S. House of Representatives unanimously passed a bill that forbids data brokers from moving certain types of Americans' sensitive personal information offshore so as to protect American national security and individual privacy. This bill was later included in a national security and foreign aid package, which was passed by both chambers of Congress and signed into law on April 24, 2024.

» ***Cybersecurity Requirements for U.S. Cloud Computing Contractors:*** Since 2015, cloud computing service providers have been required to store defense-related U.S. government data on servers on U.S. territory. In 2023, the Federal

Acquisition Regulatory Council proposed a new regulation to require the same for non-defense-related U.S. government data.

» ***Executive Order 14117 – Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern:*** In February 2024, the Biden administration issued an executive order to prevent access to Americans' bulk sensitive personal data and U.S. government-related data by countries of concern. This policy ordered the Department of Justice to issue regulations banning the acquisition, holding, use, transfer, transportation, or exportation of bulk sensitive personal data or U.S. government-related data to a foreign country of concern or a national of such a country. The Department issued its final rule in January 2025, and it becomes effective on April 8, 2025.

» ***Montana's Genetic Information Privacy Act:*** In 2023, Montana's lawmakers passed a law that bans the storage of genetic and biometric data collected in the state in countries sanctioned in any way by the U.S. federal government.

» ***2023 Amendment to California's Confidentiality of Medical Information Act:*** California legislators amended the Confidentiality of Medical Information Act to mandate in-state storage of sensitive medical information related to reproductive health and gender-affirming care, prohibiting the transfer of such information outside the state.

Each of these U.S. policies fundamentally conflicts with the notion that binding international rules should prohibit governments from the regulating cross-border data flows or data storage locations. This briefing paper shows that the exceptions to such prohibitions that have been included in existing and proposed trade deals would not ensure governments' abilities to implement these kinds of policies.

The degrees to which countries' regulation of the data economy is impeded vary greatly depending on the scope of the trade-deal rules. The chart below compares three distinct models of international data flows rules in trade pacts. The columns, from left to right, describe the features of the 2019 U.S-Mexico-Canada Agreement (USMCA); the 2021 Mercosur E-Commerce Agreement model; and the provisions from the 2022 EU-New Zealand trade agreement.

Side-by-Side Comparison of Digital Trade Data Flows Commitments in Three Key Trade Agreements

Agreement	USMCA	Mercosur	EU-New Zealand
Obligations			
Blanket prohibition on governments limiting data flows?	Yes	No	No
Prohibition on regulation applies broadly, not only to data moving between signatory countries?	Yes	Yes	No — limits on regulation apply to data flowing between the signatory countries only
Gives rights to companies/private parties?	Yes	Yes	No
Forbids data localization requirements?	Yes	Yes	Yes
Exceptions			
Defending countries must prove public interest policies meet a narrow trade pact necessity test and must satisfy a proportionality test that assesses their trade restrictiveness?	Yes	No	No (in the case of personal data and privacy)
Public interest policies must not arbitrarily or unjustifiably discriminate between countries?	Yes	Yes	Yes

Through a detailed analysis of these provisions, this policy brief shows that a potential expansion of the USMCA digital trade model would undermine existing and thwart future data-related regulation both in the United States and abroad. Indeed, changes to the USMCA rules to make them consistent with U.S. federal and state law will be a critical part of the mandatory six-year review of the USMCA, which starts this year.

The USMCA data rules (i) establish a blanket prohibition on countries restricting cross-border movements of data, explicitly including personal

data, in addition to banning data storage and processing requirements; (ii) apply beyond the signatory countries and forbid limitation on the movement of data to any country that a business operating in a signatory nation chooses; and (iii) only include a "public policy objective" exception based on deeply flawed World Trade Organization (WTO) language that has failed to preserve countries' policy space for three decades. Both the Mercosur and the EU models have more limited restrictions on government action and allow more flexibility to regulate data transfers to meet public interest objectives.

This policy brief also explains why digital trade rules on data transfers do not remedy censorship practices in non-democratic countries and related human rights violations related to online surveillance targeting vulnerable populations by authoritarian governments. First, non-democratic countries have a poor track record of adjusting their policies to trade pact commitments. Existing WTO rules already oblige signatory countries to allow the use of their communications networks to convey information on a non-discriminatory basis. This obligation is routinely ignored by countries that block access to certain news media and other websites. Second, the policies and practices actually used by authoritarian governments to limit their citizens' access to information or to surveil them would not be forbidden by proposed digital trade rules. Conversely, the promotion of privacy-first international instruments — such as the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, also known as Convention 108+ — is more likely to spotlight and help combat abusive practices.

Besides undercutting personal data protection regimes, digital trade rules that ban international data-transfer regulation and data-storage requirements could implicate government data security, tax policy, and AI regulation. Other policies that could be challenged under expansive cross-border data flows and location of computing facilities rules include:

- A Swedish law that requires a copy of accounting data to be stored locally;
- Australia's Electronic Health Records Act, which limits the foreign jurisdictions where sensitive health data can be transferred;
- An Indian insurance law that requires insurance data to be stored in domestic data centers only;
- South Korea's Land Survey Act, which prevents the unrestricted transfer of certain security-related map data outside the country;
- Potential taxes on the collection or sale of certain data, such as policies proposed in Washington state and New York;
- Data-sharing mandates, such as those included in the EU's 2018 Payment Services Directive, Data Act, Digital Services Act, and Digital Markets Act; and
- Limitations on the transfer of non-personal data outside of the EU in the Data Act and the Data Governance Act.

INTRODUCTION

Data flows. Every time we send an email, stream a video, or access an online document, data is flowing, potentially across borders. Information has been flowing internationally, through submarine cables and satellites, for decades now. The movement of data supports an array of important policy goals, including the functioning of the World Wide Web. However, recognizing the importance of the international flow of information is not the same as forbidding policies that ensure the movement of data does no harm to, and indeed furthers, public interest objectives. Important societal goals that might require the regulation of data flows include safeguarding personal privacy, ensuring data security, promoting fair digital competition, and — a more recent concern — establishing guardrails for the development and deployment of powerful artificial intelligence (AI) systems.

The very notion that there is a public interest in how data flows are governed is seen as a threat by data brokers; large online platforms like Google, Facebook, and Amazon; and other companies that profit from exploiting personal and non-personal data extracted from people and businesses across the world. Such data, generated when we use social media sites, shop online, search for information, use GPS systems, etc., reveal our preferences, locations, personal and work connections, health status, and more. The firms target advertising and sales and train artificial intelligence systems with our personal data and sell our information to others for various uses. To maximize the profits they generate from this business model based on the exploitation of our personal data, these firms seek to acquire, process, accumulate, store, and sell data however and wherever they choose without any oversight or limits, increasing their already oversized and problematic market power. They have branded their goal of obtaining unregulated control over our personal data as "free data flows" to suggest that any limitation on their control is a violation of our freedom.

However, policymakers around the world are increasingly discussing and adopting policies that govern the way in which data is collected, transferred, and stored, with the goal of meeting key public interest objectives. A vast majority of countries have personal data protection regimes with limits on the cross-border movement of data. In the United States and other countries, lawmakers and regulators are deploying national security measures that restrict or outright prohibit certain transactions involving sensitive data. Experts and advocates are exploring ways to adequately tax the data economy, and this could imply curbing international data transfers. Finally, the explosion of AI systems, trained on massive amounts of data, has raised questions about how to ensure that smaller companies have access to this critical resource, rather than it being monopolized by incumbent tech giants.

Expansive rules in international trade agreements that impose binding restrictions on governments' abilities to regulate cross-border data flows and data locations run counter to these data governance efforts. Particularly, rules that effectively guarantee private corporations unfettered rights to collect, move,

and store data wherever they choose would drastically undermine countries' abilities to regulate in the digital era.

This briefing paper shows that such extreme restrictions have adverse implications for privacy, data security (including national security concerns), tax policy, and AI regulation. The paper explores why and how countries are regulating data transfers in each of these areas and how the United States and other nations could be affected if digital trade rules that privilege corporations' imperatives over the public interest were widely adopted.

THE EMERGENT DATA GOVERNANCE ECOSYSTEM VERSUS THE DIGITAL TRADE RULES THAT LIMIT DATA TRANSFER AND STORAGE REGULATION

While fighting government oversight country by country, large tech firms profiting from the exploitation of data also launched a wholesale anti-regulation effort via trade agreements.[1] Powerful industries have used international trade deals to impose binding commitments on governments that favor their narrow commercial interests over the public interest. Since the early 1990s, with the launch of the World Trade Organization (WTO) and various free trade agreements, such pacts have been expanded beyond traditional trade matters like tariffs and quotas to include binding and enforceable constraints on signatory governments' domestic policies and to require that governments provide commercial entities certain rights and privileges. Countries are obligated to conform their domestic laws to trade pact rules, and the powerful enforcement systems these deals include, trade sanctions in particular, are effective in assuring compliance. And once agreed upon, the rules of such pacts cannot be modified except by the consensus of all signatory countries, thus providing a means to lock into place policies that residents of a country may oppose.

This is why certain tech interests advocate for trade agreements to include strong limits on governments' abilities to regulate international data transfers and data location. These terms — often included in "digital trade" or "e-commerce" chapters or agreements — usually ban government regulation of international data transfers[2] (cross-border data flows rules) and/or prohibit what industry calls "data localization"[3] (location of computing facilities rules). Data localization is a term used by the tech industry to describe an array of policies that require local storage of certain types of data, mandate the use of domestic servers in specified conditions, or impose other limits on where industry can process or store data. The industry has labeled the latter set of practices "data localization requirements." It is worth noting that industry lobbyists, allies, and analyses often conflate any kind of data-flow regulation with the concept of data localization in an attempt to delegitimize the mere notion of data governance.

Obviously, governments retaining the ability to regulate data flows does not mean that the transnational movement of information will stop, or that the internet will suddenly crash. Allowing countries to limit or regulate certain transfers of data merely recognizes that national governments are the entities with the power to enforce democratically adopted

1 David Dayen, "Big Tech Lobbyists Explain How They Took Over Washington," The American Prospect, April 18, 2023, https://prospect.org/power/2023-04-18-big-tech-lobbyists-took-over-washington/.

2 For instance, Article 19.11 of the United States-Mexico-Canada Agreement (USMCA) provides: "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."

3 USMCA Article 19.12 bans data localization requirements in the following terms: "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."

regulations to safeguard the public interest. The digital economy is no exception, even if the United States is just now catching up with other countries in acting.

Indeed, it is increasingly clear that data-exploiting industry imperatives undercut protections for citizens, governments, and smaller businesses. The U.S. government is beginning to take action to address these threats. Recent U.S. policies include:

» ***Protecting Americans' Data from Foreign Adversaries Act of 2024:*** In March 2024, the U.S. House of Representatives unanimously passed a bill that forbids data brokers from moving certain types of Americans' sensitive personal information offshore so as to protect American national security and individual privacy.[4] This bill was later included in a national security and foreign aid package, which was passed by both chambers of Congress and signed into law on April 24, 2024.[5]

» ***Executive Order 14117 – Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern:*** In February 2024, the Biden administration issued an executive order to prevent access to Americans' bulk sensitive personal data and U.S. government-related data by countries of concern.[6] This policy orders the Department of Justice to issue regulations banning the acquisition, holding, use, transfer, transportation, or exportation of bulk sensitive personal data or U.S. government-related data to a foreign country of concern or a national of such a country. The Department issued its final rule in January 2025, and it becomes effective on April 8, 2025.[7]

» ***New Cybersecurity Requirements for Cloud Computing Contractors:*** In 2023, the Federal Acquisition Regulatory Council proposed a new regulation that mandates cloud computing service providers to store non-defense-related U.S. government data on servers on U.S. territory.[8] Defense-related U.S. government data has been subject to this requirement since 2015.[9]

» ***Montana's Genetic Information Privacy Act:*** In 2023, Montana's lawmakers passed a law that bans the storage of genetic and biometric data collected in the state in

4 U.S. House, Protecting Americans' Data from Foreign Adversaries Act of 2024, HR 7520, 118th Congress, 2nd sess., introduced in House March 5, 2024, https://www.congress.gov/bill/118th-congress/house-bill/7520/.

5 See Division I—Protecting Americans' Data from Foreign Adversaries Act of 2024: U.S. House, Making Emergency Supplemental Appropriations for the Fiscal Year Ending September 30, 2024, and for Other Purposes, HR 815, 118th Congress, 1st sess., introduced in House February 2, 2023, https://www.congress.gov/bill/118th-congress/house-bill/815.

6 "Executive Order 14117, of February 28, 2024, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," Code of Federal Regulations, title 3 (2024), https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

7 Federal Register, *Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, A Rule by the Justice Department*, January 8, 2025, https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern#sectno-reference-202.301.

8 Federal Register, *Federal Acquisition Regulation: Standardizing Cybersecurity Requirements for Unclassified Federal Information System, A Proposed Rule by the Defense Department, the General Services Administration, and the National Aeronautics and Space Administration*, March 10, 2023, https://www.federalregister.gov/documents/2023/10/03/2023-21327/federal-acquisition-regulation-standardizing-cybersecurity-requirements-for-unclassified-federal.

9 U.S. Department of Defense, *Defense Federal Acquisition Regulation Supplement (DFARS)*, Sec. 239.7602-2 "Required Storage of Data within the United States or Outlying Areas," August 26, 2015, https://www.acquisition.gov/dfars/part-239-acquisition-information-technology.

countries sanctioned in any way by the U.S. federal government.[10]

» ***2023 Amendment to California's Confidentiality of Medical Information Act:*** California legislators amended the Confidentiality of Medical Information Act to mandate in-state storage of sensitive medical information related to reproductive health and gender-affirming care, prohibiting the transfer of such information outside the state.[11]

Each of these U.S. policies fundamentally conflicts with the very notion that binding international rules should prohibit the regulation of cross-border data flows or data storage locations. As this briefing paper shows, the exceptions to such prohibitions that have been included in existing and proposed trade deals would not ensure governments' abilities to adopt these kinds of policies.

Former U.S. Trade Representative Katherine Tai recognized that cementing stringent international rules about data flows and storage without first establishing U.S. domestic policies on data privacy and security would be "policy suicide."[12] She noted that Republican and Democratic members of Congress were working together to enact laws to govern data flows and establish other Big Tech–related policies, and trade law should reflect that new reality.

While U.S. policymakers grapple with this important sequencing problem, it is informative to consider the ways in which other countries with more established domestic privacy and data security rules in effect have shaped data-related terms in international pacts. With respect to the United States, there are only two agreements, the U.S-Mexico-Canada Agreement (USMCA) and a deal with Japan, that include the binding and expansive constraints on data regulation promoted by industry lobbyists. In contrast, other countries' agreements include terms that provide more policy space to allow public interest regulation.

The chart below compares three distinct models of international data-flow commitments. The columns, from left to right, describe the features of the 2019 USMCA; the 2021 Mercosur E-Commerce Agreement model; and the provisions from the 2022 EU-New Zealand trade agreement, which represent a 2018 "horizontal" EU position on data flows agreed between the European Parliament and Commission to be included in all EU agreements.

Regarding the agreements' language on data flows and location of computing facilities, there are two levels of focus: (i) the "obligations" with which countries agree to conform their domestic law; and (ii) the exceptions to those obligations, which may protect policies that would otherwise conflict with the obligations. (For a detailed analysis of the texts, please see the Appendix.)

10 Legislature of the State of Montana, Genetic Information Privacy Act, SB 351, introduced in Assembly February 15, 2023. https://bills.legmt.gov/#/bill/20231/LC1085?open_tab=sum.

11 California Legislature, Health Information, AB 352, introduced in Assembly January 31, 2023, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB352.

12 David Westin, "Fireside Chat with Katherine Tai," interview by David Westin, The Aspen Institute, video, December 7, 2023, https://www.youtube.com/watch?v=nwT5GfbxTMY&t=186s.

Side-by-Side Comparison of Digital Trade Data Flows Commitments in Three Key Trade Agreements

Agreement	USMCA	Mercosur	EU-New Zealand
Obligations			
Blanket prohibition on governments limiting data flows?	Yes	No	No
Prohibition on regulation applies broadly, not only to data moving between signatory countries?	Yes	Yes	No — limits on regulation apply to data flowing between the signatory countries only
Gives rights to companies/private parties?	Yes	Yes	No
Forbids data localization requirements?	Yes	Yes	Yes
Exceptions			
Defending countries must prove public interest policies meet a narrow trade pact necessity test and must satisfy a proportionality test that assesses their trade restrictiveness?	Yes	No	No (in the case of personal data and privacy)
Public interest policies must not arbitrarily or unjustifiably discriminate between countries?	Yes	Yes	Yes

A thorough analysis of these provisions leads to the conclusion that a potential expansion of the USMCA model would thwart data-related regulation both in the United States and abroad.

The USMCA data rules:

» establish a blanket prohibition on restrictions of cross-border movements of data, explicitly including personal data, in addition to banning data storage and processing requirements;

» apply beyond the signatory countries and forbid limitation on the movement of data to any country that a business operating in a signatory nation chooses; and

» only include a "public policy objective" exception based on the deeply flawed WTO language, which has failed to preserve countries' policy space for three decades.[13]

Both the Mercosur and the EU models have more limited commitments and allow more flexibility to regulate data transfers to meet public interest objectives. Fortunately, the USMCA language is an anomaly relative to the digital or e-commerce terms that have been included in some U.S. trade pacts since 2004. These past U.S. pacts do not include the extreme industry-favored language.

Considering this changing landscape, it is not surprising that in 2023 the U.S. government decided to withdraw its support for a 2019 proposal to include the USMCA cross-border data flows and location of computing facilities language in the E-Commerce Joint Statement Initiative (JSI).[14] The JSI is an agreement that a subset of WTO nations have been negotiating since 2017. These negotiations are arguably the most important ongoing digital trade talks, as they involve over 90 countries and, given the proponents' objective of linking them to the WTO structure and its dispute settlement system, could be enforceable with sanctions. After years of deadlock, in the summer of 2024, the proponents of this agreement announced the completion of a "stabilized text" for the first tranche of the agreement. The U.S. decision to withdraw support for the 2019 data proposals broke the JSI impasse by making clear that there was insufficient agreement among countries to include terms related to data transfers in the first tranche. Yet the new text, without data-flow obligations, that Singapore, Japan, and Australia — the countries leading the JSI talks — drafted still does not have the support of all countries participating in the negotiations. (Among the problems that the U.S. government has noted is the text's lack of an effective security exception.) Thus, a bloc of countries, including the United States, have expressed reservations over the stabilized text. The legal status of this document is uncertain.[15]

13 Daniel Rangel, "WTO General Exceptions: Trade Law's Faulty Ivory Tower," Public Citizen's Global Trade Watch, last modified February 4, 2022, https://www.citizen.org/article/wto-general-exceptions-trade-laws-faulty-ivory-tower/. Countries' attempts to defend their domestic policies using the language included in the public policy exception have failed in 46 of 48 attempted uses since the establishment of the WTO.

14 David Lawder, "US Drops Digital Trade Demands at WTO to Allow Room for Stronger Tech Regulation," Reuters, October 25, 2023, https://www.reuters.com/world/us/us-drops-digital-trade-demands-wto-allow-room-stronger-tech-regulation-2023-10-25/.

15 Peter Ungphakorn, "Getting to Yes: What's Behind the E-Commerce Standoff at the WTO?," Hinrich Foundation, last modified August 13, 2024, https://www.hinrichfoundation.com/research/wp/wto/what-is-behind-the-e-commerce-standoff-at-the-wto/.

Cross-Border Data-Flow Rules in Trade Agreements Will Not Preserve the Ideal of a Free and Open Internet

Certain civil liberties groups concerned with censorship practices in non-democratic countries have expressed concern about the U.S. government's decision to withdraw support for 2019 data flows and location of computing facilities proposals at the WTO. In their view, using trade agreements to limit the regulation of data flows could protect vulnerable populations from authoritarian governments. These groups believe that, without trade agreement rules protecting data flows, authoritarian governments could mandate data localization as a means to gather potentially harmful information about political opponents, journalists, and activists. They also assert that free-data-flow guarantees could prevent the internet from breaking apart via government-imposed digital censorship regimes.[16]

While concerns regarding authoritarian models for the internet and online censorship are legitimate, these groups' aspiration to find solutions in trade deals is misplaced. Digital trade rules will not stop authoritarian governments from limiting access to news media and other websites or prevent online snooping on journalists, opponents, activists, and rights defenders. The digital trade rules in question are not designed to do so.[17] And, even if they were, non-democratic countries have a poor track record of adjusting their policies to trade pact commitments. By contrast, digital trade rules banning data-transfer regulation are likely to undermine domestic regulation in democratic countries that place greater value in international law.

Key elements of China's and Russia's so-called "cyber sovereignty" projects are not disciplined by bans on the regulation of data transfers. Policies banning certain social networks or media outlets, such as those adopted in China and Russia for years, go far beyond limiting the cross-border flow of data. They basically ban certain applications from operating using a country's national networks. It is worth noting that, since 1994, WTO member countries have had an obligation to allow service suppliers of any other WTO signatory to use

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

17 Kristina Irion, Margot E. Kaminski, and Svetlana Yakovleva, "Privacy Peg, Trade Hole: Why We (Still) Shouldn't Put Data Privacy in Trade Law," The University of Chicago Law Review Online, March 27, 2023, https://lawreviewblog.uchicago.edu/2023/03/27/irion-kaminski-yakovleva/.

telecommunications networks and services for the movement of information within and across borders.[18] However, this obligation neither prevented China from keeping and expanding its Great Firewall, which blocks access to blacklisted foreign websites and services, when it acceded to the WTO in 2001 nor impeded Russia's decision to ban Western social media networks and news outlets after its invasion of Ukraine in 2022.[19] After years of violating their existing WTO obligations regarding access to telecommunications networks, it is highly unlikely that these countries will stop their censorship practices because new trade pact obligations obstruct data regulation.

With respect to concerns that authoritarian governments will use data localization requirements to snoop on or threaten journalists, political leaders, rights advocates, or activists, unfortunately, governments with such intentions do not need data to be stored locally in order to surveil their targets. Amnesty International, for instance, has exposed how both non-democratic and democratic governments have used Israeli company NSO Group's Pegasus surveillance technology to snoop on journalists, political opponents, and more. Such spyware technology works regardless of where data is stored and is able to access a victim's messages, emails, media, microphone, camera, calls, and contacts just by infecting the victim's device.[20] Notably, Amnesty International does not advocate against local data storage laws. Rather, it urges countries to adopt a global moratorium on the sale, transfer, export, and use of spyware.[21]

In the event that data localization laws are abused to violate rights,[22] advocates should promote instruments that prioritize human rights instead of commercial interests. The most salient of such international instruments is the Convention for the Protection of Individuals with Regard to the Processing of Personal Data,

18 Section 5(c), Annex on Telecommunications, WTO General Agreement on Trade in Services.
19 Elena Zinovieva and Bai Yajie, "Digital Sovereignty in Russia and China," Modern Diplomacy, July 31, 2023, https://moderndiplomacy.eu/2023/07/31/digital-sovereignty-in-russia-and-china/.
20 "Massive Data Leak Reveals Israeli NSO Group's Spyware Used to Target Activists, Journalists, and Political Leaders Globally," Amnesty International, last modified July 19, 2021, https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/.
21 "The Pegasus Project: One Year On, Spyware Crisis Continues After Failure to Clamp Down on Surveillance Industry," Amnesty International, last modified July 18, 2022, https://www.amnesty.org/en/latest/news/2022/07/the-pegasus-project-one-year-on-spyware-crisis-continues-after-failure-to-clamp-down-on-surveillance-industry/.
22 Adrian Shahbaz, Allie Funk, and Andrea Hackl, "User Privacy or Cyber Sovereignty?," Freedom House, accessed November 1, 2024, https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty.

also known as Convention 108+. This agreement, developed under the auspices of the Council of Europe, has been signed by 46 European countries plus eight non-European nations such as Argentina, Mexico, Morocco, Senegal, and Uruguay.[23] Convention 108+ establishes a floor of personal data protection that has been described by experts as "GDPR lite,"[24] making reference to the EU's General Data Protection Regulation, which is described in detail below. This international pact regulates data processing, including personal data collection by public entities, and mandates that such processing be proportionate, legitimate, and lawful. Moreover, this agreement also includes rules on cross-border flows of personal data. However, it does so in a way that prioritizes data protection and requires that countries ensure cross-border data transfers do not lead to the circumvention of the guarantees included in the convention. This model is much more likely to find the right balance between personal data protection and the cross-border movement of information. Privacy groups in the United States have advocated for a U.S. accession to Convention 108+.[25] Civil liberties advocates should follow their lead and promote other countries' accession to this privacy-first agreement.

23 "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data," opened for signature January 28, 1981, European Treaty Series no. 108, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108.
24 Graham Greenleaf, "Convention 108+ and the Data Protection Framework of the EU," University of New South Wales Law Research Series, no. 18–39 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3202606.
25 Electronic Privacy Information Center, April 13, 2018, letter to U.S. Senate Committee on Foreign Relations, https://archive.epic.org/EPIC-SFR-Pompeo-April2018.pdf.

While the status of the WTO JSI on E-Commerce is uncertain, efforts to insert binding restrictions on governments' abilities to regulate cross-border data flows in international trade agreements abound. Thus, policymakers and trade negotiators must be aware of the myriad domestic regulatory goals that could be undermined or otherwise implicated by this set of rules.

The rest of this briefing paper shows that such restrictions have adverse implications for privacy, data security (including national security concerns), tax policy, and AI regulation. Each of the following sections first explores why and how countries are regulating data transfers in each of these areas, then lays out how the United States and other nations could be affected if digital trade rules that privilege corporations' imperatives over the public interest were widely adopted.

HOW DIGITAL TRADE RULES CAN ENDANGER POLICIES ENSURING THE RIGHT TO PRIVACY

Digital platforms and other tech firms have developed business models based on the use and sale of data, including our personal data. To maximize their profits and convenience, they seek unregulated cross-border data flows so that they can process, store, and sell data without any constraints. They have branded the concept as "free data flows" for their advocacy efforts. Although the exchange of data fosters knowledge sharing and global connectivity, there are valid grounds for regulating data collection, processing, transmission, storage locations, and retention periods, especially for certain data types.

The rise in the generation, use, and sale of large amounts of data in the digital economy has led to the pervasive practice of commercial surveillance, where every click and every search is tracked for targeted advertising and other rent-seeking practices. Information collected for such commercial purposes leads to negative spillover effects. Data-based targeting has led to most advertising revenue flowing toward dominant platforms, making it difficult for users and advertisers to switch to new competitors. In this way, dominant platforms maintain their monopolistic hold over digital markets.[26] They also overtake other services, such as news media, as advertising that would otherwise have accrued to support journalism is now gobbled up by tech giants. Excessive data collection enables some of the most problematic aspects of social media applications, which are contributing to a youth mental health crisis, according to the U.S. Surgeon General.[27]

As a result, many countries around the world have begun trying to protect people's rights to control their personal information through privacy legislation. But the intangibility and mobility of digital data poses regulatory challenges given the territorial nature of regulatory sovereignty and governance. Many countries have instituted restrictions or conditions on the cross-border transfer of data to try to ensure that their citizens' privacy rights are not compromised simply by moving the residents' personal data to another country.

Of the 193 countries recognized by the United Nations, 162 have passed national personal data protection laws.[28] About 75% of all countries have adopted some conditions on the cross-border transfer of data.[29] See the figure below. Only a handful of countries have no conditions or limitations on cross-border data transfers.

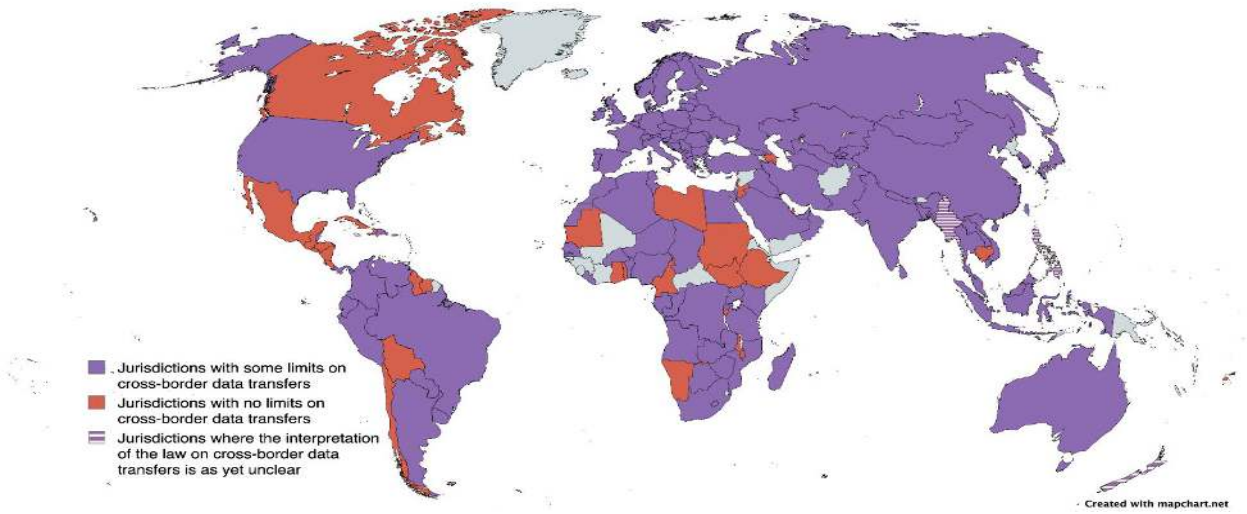
26 U.S. House, Committee on the Judiciary, Subcommittee on Antitrust, Commercial and Administrative Law, Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations, 116th Congress, 2nd sess., 2020, Committee Print 117-8, https://democrats-judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf.

27 Vivek H. Murthy, "Surgeon General: Why I'm Calling for a Warning Label on Social Media Platforms," New York Times, June 17, 2024, https://www.nytimes.com/2024/06/17/opinion/social-media-health-warning.html.

28 Graham Greenleaf, "Global Data Privacy Laws 2023: 162 National Laws and 20 Bills," 181 Privacy Laws and Business International Report (PLBIR) 1, 2-4, UNSW Law Research Paper no. 23–48 (2023), https://ssrn.com/abstract=4426146 or http://dx.doi.org/10.2139/ssrn.4426146.

29 Satyajit Parekh, Stephen Reddin, Kayvaun Rowshankish, Henning Soller, and Malin Strandell-Jansson, "Localization of Data Privacy Regulations Creates Competitive Opportunities," McKinsey & Company, last modified June 30, 2022, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities.

Figure 1. Countries' International Data-Transfer Policies



Source: Compiled by the authors based on data from U.S. Department of State Investment Climate Statements 2023 and DLA Piper's repository of data protection laws around the world. Created using mapchart.net. In Canada, there are specific limitations on the transfer of some kinds of data outside Québec[30] and Ontario.[31]

For instance, Brazil's Lei Geral de Proteção de Dados Pessoais (LGPD) allows for the cross-border transfer of personal data only when the receiving country has an adequate level of personal data protection, with a few exceptions.[32] Similar adequacy clauses in the UK's Data Protection Act of 2018 allow the country to choose which jurisdictions can receive personal data from UK citizens.[33] Under Kenya's Data Protection Act, transfers of personal data outside of Kenya can only take place under any one of the following circumstances: (i) the data controller or data processor can provide appropriate data protection safeguards; (ii) an adequacy decision has been made by the data commissioner; (iii) the transfer is necessary to fulfill a set of limited objectives, such as protecting the vital interests of the data subject; or (iv) the data subject has given consent.[34]

The European Union's General Data Protection Regulation (GDPR) is arguably a global high standard for personal data protection. It allows for personal data transfer only to jurisdictions with a certain level of data protection.[35] The European Commission makes these decisions on the basis of an "adequacy" determination, which provides that the countries where the

30 Candice Hévin and Simon Du Perron, "Cross-Border Transfers of Personal Information Outside Québec: Requirements for Businesses," Borden Ladner Gervais LLP, last modified May 7, 2024, https://www.blg.com/en/insights/2022/12/cross-border-transfers-of-personal-information-outside-quebec.

31 Candice Teitlebaum and Aaron Collins, "Canadian Privacy Legislation and the Cross-Border Transfer of Personal Information Part One: Personal Health Information," Aird & Berlis LLP, last modified May 2008, https://www.airdberlis.com/docs/default-source/articles/article---cross-border-transfer-of-personal-health-information.pdf?sfvrsn=2.

32 Lei Geral de Proteção de Dados Pessoais (LGPD), Article 33 I of Law No. 13.709 (2018), Government of Brazil, https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm.

33 Data Protection Act 2018, Sections 73 and 74, UK Public General Acts (2018), https://www.legislation.gov.uk/ukpga/2018/12/section/73/enacted.

34 The Data Protection (General) Regulations, Part VII, Kenya Gazette Supplement No. 236 (2021), https://www.odpc.go.ke/wp-content/uploads/2024/03/THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021-1.pdf.

35 General Data Protection Regulation (GDPR), Official Journal of the European Union (2016), Article 45(3), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

data can be freely transferred have a level of privacy protection equivalent to that of the EU. If no such adequacy determination is made, data can be transferred outside the EU under binding corporate rules for intra-company transfers or standard contractual clauses for inter-company transfers. The liability for breaches, however, remains with the EU entity carrying out the transfer.[36] In practice, companies widely use such standard contractual clauses to transfer data out of the EU.[37]

As of 2024, the European Commission has recognized Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom, the United States (only for commercial organizations participating in the EU-US Data Privacy Framework[38]), and Uruguay as providing adequate protection such that data can flow freely between the EU and these jurisdictions without additional safeguards.[39]

The EU's Model to Safeguard Privacy From Trade Pact Obligations

Privacy is considered a basic human right in the European Union. Before the GDPR, data-related privacy rights in the EU were governed by the 1995 Data Protection Directive.[40] It established conditions for lawful data processing, individuals' personal data protection rights, and principles of data quality. In 2009, the European Commission reviewed this directive in light of the increased use by economic actors and public authorities of digital data as well as, interestingly, the spread of cloud computing.[41] The European Commission deemed that cloud computing (computing over remote servers) might involve "the loss of individuals' control over their

40 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, Official Journal of the European Union (1995), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.

41 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union, European Commission (2010), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF.

36 GDPR, Article 47.2(f); Commission Implementing Decision (EU) 2021/914: On Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, Official Journal of the European Union (2021), Clause 12(b), https://publications.europa.eu/resource/cellar/55862dbf-c72b-11eb-a925-01aa75ed71a1.0006.01/DOC_1.

37 Svetlana Yakovleva and Kristina Irion, "Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation," American Journal of International Law 114, no. 10 (2020): 10–14, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3524245.

38 The adequacy finding for the United States is premised on self-certification systems and the Biden Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities. The European Court of Justice invalidated previous U.S. adequacy findings and has not yet ruled on the latest version.

39 "Adequacy Decisions: How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection," European Commission, accessed October 28, 2024, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

potentially sensitive information when they store their data with programs hosted on someone else's hardware."[42] Underlying the review was an assumption by the European Commission that personal data protections for EU citizens should not change depending on where their data happens to be stored or processed. The Commission decided then to examine how citizens could be granted the same degree of protection as was required within the EU when their data was stored in a third country.[43]

Under the Data Protection Directive, other countries' policies and practices were assessed to determine if they provided adequate privacy protection. Based on these rules, the European Commission issued both the Safe Harbor decision in 2000 and the EU-U.S. Privacy Shield in 2016, which allowed the transfer of European personal data to certain U.S.-based companies. Both of these determinations were struck down by the Court of Justice of the European Union on the grounds that U.S. surveillance laws do not limit personal data requests to what is strictly necessary and proportionate. At the same time, the Commission became concerned about the lack of clear criteria in the Directive to guide adequacy decisions, as well as the fact that — under the Directive — both the Commission and individual Member States could grant adequacy decisions, which could lead to conflicting outcomes.[44]

The 2009 review resulted then in proposed changes to the adequacy regime for international data transfers, including a new requirement to review the third country's legal system based on a clear set of parameters. Basically, the Commission proposed that in order to grant an adequacy decision, it would have to review the following aspects of the third country's legal system: (i) public security, defense, national security and criminal laws with regard to access of public authorities to personal data; (ii) whether the jurisdiction grants effective and enforceable individual rights and effective administrative and judicial redress; and (iii) the existence and effective functioning of one or more independent supervisory authorities in the foreign jurisdiction. These changes were ultimately included in the 2016 GDPR as the successor to the Directive's EU policy on data privacy.[45]

42 Communication from the Commission: A Comprehensive Approach on Personal Data Protection, 2010.
43 Communication from the Commission: A Comprehensive Approach on Personal Data Protection, 2010.
44 Communication from the Commission: A Comprehensive Approach on Personal Data Protection, 2010: 15.
45 Article 45(2)(a) and (b) of the EU's General Data Protection Regulation.

It quickly became clear that there was a tension between the inclinations of the European Commission division negotiating trade agreements, the Directorate-General for Trade, or "DG Trade," which was supportive of the industry demand for unrestricted cross-border data flows, versus the privacy-first GDPR.[46] In particular, a 2016 study by professors Kristina Irion, Svetlana Yakovleva, and Marija Bartl clarified that the applicable WTO general exceptions language, which is replicated in many other trade pacts, would not protect the GDPR and the privacy rights it provided from conflicting with the expansive "data free flows" commitments being contemplated in various trade negotiations.[47] This study triggered an EU-wide debate over trade and privacy, with the European Parliament being intensively involved in the development of a new approach. In 2018, the European Commission adopted a new position often referred to as the "EU's horizontal provisions on cross-border data flows and personal data protection." It is the basis for the EU's 2019 proposed text on data flows and storage at the JSI negotiations.[48]

This approach includes language like that found in the 2012 U.S.-Korea Free Trade Agreement, which calls on parties to enable cross-border data transfers but does not include the USMCA language banning restrictions on transfers.[49] However, the EU horizontal provisions also include binding language that explicitly forbids specific enumerated forms of data localization requirements. This includes bans on, among others, requiring the use of computing facilities or network elements in the signatory's territory for data processing or requiring the localization of data in the signatory's territory (see Appendix for exact language). GDPR does not require the localization of EU residents' data in the EU; instead, it regulates the conditions under which data can be transferred to select countries. This means that, in principle, the ban on data localization practices should not compromise the GDPR. However, to create ironclad protections for

46 Svetlana Yakovleva and Kristina Irion, "Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade," International Data Privacy Law 10, no. 3 (2020): 201–221, https://doi.org/10.1093/idpl/ipaa003.

47 Kristina Irion, Svetlana Yakovleva and Marija Bartl, "Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements," Institute for Information Law, University of Amsterdam, https://dare.uva.nl/search?identifier=2a4a80a7-fcb3-4ee9-8b01-11a2e2cdf17a.

48 World Trade Organization, "Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce," INF/ECOM/22, April 26, 2019, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/22.pdf&Open=True.

49 Joint Statement on E-Commerce: EU Proposal, Sec. 2.7.1.

GDPR's data privacy guarantees and to safeguard policy space for any other future privacy policy that may employ different mechanisms, the horizontal provisions also include an effective exception for personal data protection and privacy policies: "Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards."[50]

The first pact to fully include this model was the EU-New Zealand free trade agreement (FTA), signed in 2022. Before, in 2021, the EU and the UK signed their post-Brexit trade and cooperation agreement, but this deal departed slightly from the horizontal provisions in terms of the exception language.[51] The EU-New Zealand agreement, however, includes the full privacy exception as drafted in the horizontal provisions.[52] It also provided for a review of this section in three years with a commitment from the New Zealand government to include Māori in the review process.[53]

In 2022, the EU and Japan decided to start negotiations on data transfers in the context of their Economic Partnership Agreement.[54] In 2023, a deal was announced.[55] The new text departs in important ways from the EU horizontal provisions and can be perceived as a backsliding with respect to deals the EU had negotiated both with the UK and New Zealand. First, the EU-Japan deal includes more prohibitions than those proposed by the horizontal provisions, such as a ban on requiring the approval of a government entity prior to the transfer of information to the territory of the other party. Moreover, the new text adds conditions that a government would have to meet in order to avail itself

50 "Horizontal Provisions on Cross-Border Data Flows and Personal Data Protection," European Commission, last modified May 18, 2018, https://ec.europa.eu/newsroom/just/items/627665.
51 "EU-UK Trade and Cooperation Agreement," conclusion date: December 30, 2020, European Commission, Art. 202, https://commission.europa.eu/strategy-and-policy/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement_en.
52 "Free Trade Agreement Between the European Union and New Zealand," conclusion date: July 9, 2023, European Commission, Ch. 12, Sec. B, Art. 12.5, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202400229#page=99.
53 "FTA Between the EU and New Zealand," Ch. 12, Sec. B, Article 12.4.
54 "Landmark EU-Japan Data Deal One Step Closer to Ratification," European Commission, last modified December 1, 2023, https://policy.trade.ec.europa.eu/news/landmark-eu-japan-data-deal-one-step-closer-ratification-2023-12-01_en.
55 "EU and Japan Conclude Landmark Deal on Cross-Border Data Flows at High-Level Economic Dialogue," European Commission, last modified October 27, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5378.

of the privacy exception. Specifically, to qualify for the exception, a privacy policy must enable international data transfers under conditions of general application, which must be formulated in objective terms. The immediate consequences of these terms might not seem especially problematic given that the EU has deemed that Japan has an adequate level of data protection, creating a de facto system of unrestricted personal data transfers in any case.[56] However, if the EU eventually decided to revoke the adequacy determination for Japan due to changes in Japan's data protection regime or stricter GDPR enforcement particularly regarding onward data transfers to third countries,[57] Japan could successfully challenge such a decision based on the new data-transfer deal.

56 "European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows," European Commission, last modified January 22, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421.

57 See Svetlana Yakovleva, "Scope and Applicability of Free Data Flow Exceptions in US-Japan Digital Trade Agreement and the CPTPP," Digital Trade Alliance Japan's 'Data Free Flow with Trust' Versus Digital Trade Agreement Commitments series (2023), https://dtalliance.org/wp-content/uploads/2023/02/Scope-and-Applicability-of-Free-Data-Flow-Exceptions-in-US-Japan-Digital-Trade-Agreement-and-the-CPTPP.pdf.

Many of the governments that retain policy space for domestic storage requirements for some kinds of data do not, as a rule, advocate for extensive data localization. For instance, the African Union's Data Policy Framework of 2022 discourages data localization but recognizes that very specific localization requirements for some sensitive categories of data agreed upon through multi-stakeholder consultations can be instituted. It also recommends that such measures be evaluated for potential harm to human rights.[58]

The tech industry's claims of alleged rising barriers to cross-border data flows are disingenuous. Given that the regulation of international data transfers is a relatively new policy concern, countries, naturally, are just now starting to adopt policies in this domain. Compared with mature industries such as heavy metals manufacturing, the number of alleged "barriers to trade" are still very low. For instance, in 2021, the Information Technology and Innovation Foundation, a Big Tech-funded think tank, sounded the alarms because it identified 144 "data flows restrictions" adopted by 62 countries worldwide.[59] This number pales in comparison with alleged trade restrictions adopted in traditional sectors. For instance, between 2009 and 2021, the University of Saint Gallen's Global Trade Alert database on trade policy interventions documented 769 potentially trade-restrictive measures adopted by countries

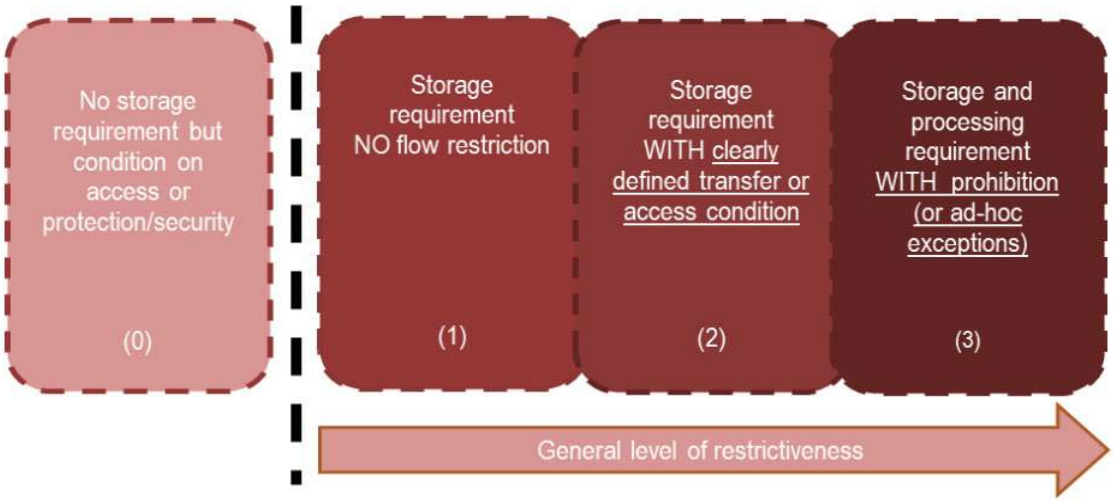
58 Mercy King'Ori, Ulric Quee, and Hunter Dorwart, "The African Union's Data Policy Framework: Context, Key Takeaways, and Implications for Data Protection on the Continent," Future of Privacy Forum, last modified March 29, 2023, https://fpf.org/blog/the-african-unions-data-policy-framework-context-key-takeaways-and-implications-for-data-protection-on-the-continent/.

59 Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," Information Technology and Innovation Foundation, last modified July 1, 2021, https://www2.itif.org/2021-data-localization.pdf.

concerning solely iron and steel products.[60] Yet iron and steel exports worldwide reached $586 billion in 2021, increasing by $170 billion compared to 2017.[61] This clearly indicates that policies perceived as "trade barriers" might affect international exchanges but by no means halt trade flows.

Moreover, governments that have adopted domestic storage requirements have chosen to calibrate the strictness of their policies depending on their desired level of protection. An OECD report shows that countries' restrictions on cross-border data transfers fall on a spectrum.[62] Sometimes, governments require only that a copy of the data be stored locally so as to make it available for government inspection, with no restriction on other copies being stored in foreign data centers. Sweden's Accounting Act is an example of this.[63] Some laws require that a copy be stored locally and that other copies be stored only in jurisdictions considered appropriate or safe — for instance, Australia's Electronic Health Records Act.[64] Other laws require that certain categories of data be stored only domestically — for instance, India's insurance law requires that all insurance data be stored in domestic data centers only.[65]

Figure 3. OECD Typology of Data Localization Measures and Requirements for Data Flows



Note: Figure is schematic; elements do not singularly identify any given country's approach to data localisation. Different approaches tend to apply to different types of data, even within a same jurisdiction.

Source: OECD.[66]

60 "Global Dynamics," Global Trade Alert, accessed November 21, 2024, https://www.globaltradealert.org/global_dynamics/area_goods/year-to_2021/day-to_1126.
61 "World Trade Statistical Review 2022," World Trade Organization, https://www.wto.org/english/res_e/booksp_e/wtsr_2022_e.pdf.
62 Javier López González, Francesca Casalini, and Juan Porras, "A Preliminary Mapping of Data Localisation Measures," OECD Trade Policy Papers, no. 262 (2022), https://doi.org/10.1787/c5ca3fed-en.
63 González, Casalini, and Porras, "A Preliminary Mapping."
64 González, Casalini, and Porras, "A Preliminary Mapping."
65 IRDAI (Maintenance of Insurance Records) Regulations, The Gazette of India (2015), Paragraph 3(9), https://irdai.gov.in/document-detail?documentId=604674.
66 González, Casalini, and Porras, "A Preliminary Mapping."

Other countries have tried to promote voluntary systems for conditions on cross-border data transfers. For instance, the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules System (CBPR) is an opt-in privacy code of conduct for companies located in APEC member countries.[67] In 2022, the U.S. Department of Commerce announced that this system would evolve into a "Global CBPR Forum" open to other countries, but it remains unclear whether the initiative will gain traction.[68] Under CBPR, participating countries have to demonstrate that privacy rules meeting the CBPR's standards are legally enforceable in their own jurisdictions. However, these standards are relatively weak. For example, they require data collectors to limit data collection to specific purposes and to inform individuals when their data is being collected.[69] Unlike stricter data protection regimes, companies are not required to minimize data collection nor prohibited from transferring specific types of sensitive information to third parties. Under this framework, companies can be certified as CBPR-compliant by third-party private firms, called accountability agents, by demonstrating that they meet the CBPR privacy standard. The CBPR does not institute binding and comprehensive conditions on cross-border data transfers. Unlike the GDPR, the conceptual basis of the CBPR is not protection of human rights but rather protection against individual risk or harm, like in tort law.[70] The CBPR does not protect personal data that is not directly collected from data subjects, and its purpose limitations are very broad.[71] Other protections in the CBPR are similarly diluted in comparison to the GDPR.[72] In fact, all countries approved to participate in the CBPR (except the United States) already have stronger data privacy laws than the APEC CBPR regime. Given the CBPR's relatively low standards compared to the domestic privacy laws of most countries, the system has largely failed to meet its goal of facilitating data transfers among participating economies.[73] These aspects make the CBPR an uncertain and generally weak data protection framework.

Acknowledging the weakness of voluntary schemes such as CBPR is relevant because under most cross-border data movement and location of computer facilities digital trade rules, even flexible conditions on data transfers or soft local storage requirements could be deemed inconsistent with trade pact commitments. Indeed, under the USMCA model described above, any kind of restriction on the movement of data across borders would be a violation of the cross-border data-flow rule. This includes privacy regimes like GDPR or the similar laws adopted by dozens of countries worldwide. Moreover, even a flexible policy like Sweden's Accounting Act, which requires a copy of accounting data be stored locally without restricting the possibility of other copies being

67 "The APEC Cross-Border Privacy Rules (CBPR) System," Asia-Pacific Economic Cooperation Cross Border Privacy Rules System, accessed March 21, 2024, https://cbprs.org/.
68 Graham Greenleaf, "Global CBPRs: A recipe for failure?," University of New South Wales Law & Justice Research Series, 177 Privacy Laws & Business International Report 11–13 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4180516.
69 "Template Notice of Intent to Participate in the APEC Cross Border Privacy Rules System," Asia-Pacific Economic Cooperation Cross Border Privacy Rules System, last modified November 2019, https://cbprs.org/wp-content/uploads/2019/11/6.-Template-Notice-of-Intent-to-Participate-in-the-CBPR-System-updated-17-09-2019.pdf.
70 Clare Sullivan, "EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era," Computer Law & Security Review 35, no. 4 (2019): 380–397, https://doi.org/10.1016/j.clsr.2019.05.004.
71 Sullivan, "EU GDPR or APEC CBPR?"
72 Sullivan, "EU GDPR or APEC CBPR?"
73 Greenleaf, "Global CBPRs: A recipe for failure?"

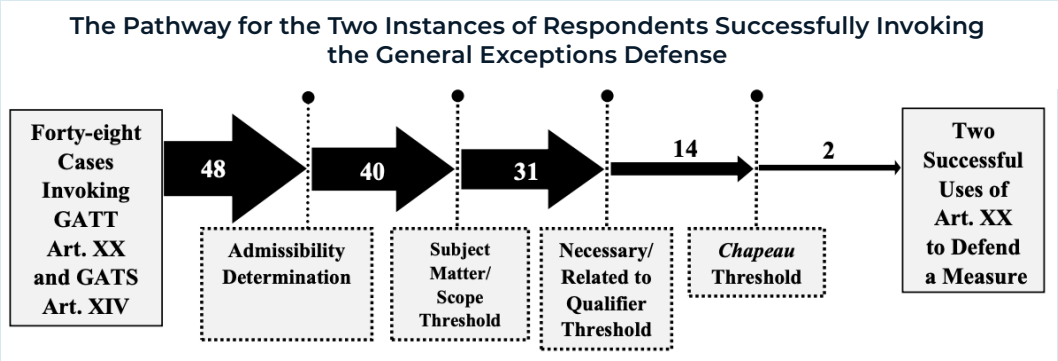
stored in foreign data centers, would be a data localization requirement banned by most digital trade rules on data storage. The expansive nature of these prohibitions and, as explained in the box below, the way in which the balance between data protection and unhindered movement of data in most existing digital trade agreements is skewed toward the latter means that countries could be forced to adopt less protective domestic privacy regimes if they want to comply with digital trade rules.

So-called "public policy" exceptions based on the WTO's GATT/ GATS general exception undermine countries' capacities to choose their desired level of data protection

The USMCA model for rules on "cross-border data flows" imposes strict constraints on governments' rights to regulate data flows with a specific exception based on the WTO General Agreement on Tariffs and Trade (GATT) and General Agreement on Trade in Services (GATS) general exceptions. Over the years, scores of trade tribunal rulings have proven these exceptions to be largely ineffective. Tribunals have ruled against the use of GATT and GATS general exceptions to defend countries' domestic policies in 46 of 48 attempts since the WTO started in 1995.[74]

One of the main issues with the WTO model for exceptions language is the use of proportionality tests to assess the trade restrictiveness of a policy. Some WTO exceptions only allow countries to justify public interest policies under the exceptions when they are "necessary" to meet their public interest goal. This means that if policymakers or regulators opt for policies that a trade tribunal concludes are "more restrictive than necessary," the policies cannot be justified under the exceptions. This requirement was incorporated in USMCA's terms on cross-border data flows and a number of other agreements (see Appendix for the specific language).

74 Daniel Rangel, "WTO General Exceptions: Trade Law's Faulty Ivory Tower," Public Citizen's Global Trade Watch, last modified February 4, 2022, p. 18–19, https://www.citizen.org/wp-content/uploads/WTO-General-Exceptions-Paper_-1.pdf.



Source: Public Citizen.[75]

In the context of data policies, for instance, if a country chooses to require that copies of sensitive health data are stored locally and that copies of such data are only stored in jurisdictions considered appropriate or safe, like Australia does, another country could claim that this limitation on the cross-border movement of data is more restrictive than necessary. The challenging country could argue that Australia should rely on less restrictive policies, like only requiring that a copy of health data is stored locally without regulating whether other copies are stored abroad or trusting companies' compliance with the weak APEC CBPR framework. If a trade tribunal agrees with that argument — and, as the chart above shows, many attempted uses of the exception language have failed on this very test — Australia's policy would not be safeguarded by the exception and would be deemed inconsistent with the trade agreement. A ruling against such data policy could expose the regulating country to millions in retaliatory tariffs that stay in place until the policy is changed, which in turn could put pressure on policymakers and regulators to roll back or weaken the policy.

75 Rangel, "WTO General Exceptions."

In the United States, there is a growing interest in privacy legislation at the state level due to difficulties in passing federal privacy legislation. In 2023, Montana's lawmakers passed a law that bans the storage of genetic and biometric data collected in the state in countries sanctioned in any way by the United States Office of Foreign Asset Control or designated as a foreign adversary.[76] In 2023, California legislators amended the Confidentiality of

76 Legislature of the State of Montana, Genetic Information Privacy Act, SB 351, introduced in Assembly February 15, 2023. https://bills.legmt.gov/#/bill/20231/LC1085?open_tab=sum.

Medical Information Act to mandate in-state storage of sensitive medical information related to reproductive health and gender-affirming care, prohibiting the transfer of such information outside the state.[77] If the digital trade rules advocated by Big Tech were widely implemented, these policies' restrictions on data movement across state lines would conflict with the digital trade prohibition on regulating cross-border data flows and local storage requirements.

While preserving states' capacities to enforce their privacy laws is of the utmost importance, guaranteeing policy space for federal privacy safeguards is also essential. In April 2024, House Energy and Commerce Chair Cathy McMorris Rodgers (R-WA-05) and Senate Commerce Chair Maria Cantwell (D-WA) unveiled a new comprehensive federal privacy bill. The American Privacy Rights Act (APRA) was Congress' latest bipartisan attempt to implement a nationwide data-related privacy law. The APRA would impose obligations on "covered entities" and, in some cases, "service providers" to protect Americans' right to privacy. While APRA does not have explicit limitations on international data transfers, its enforcement would likely require such limits in specific cases. For instance, under APRA, covered entities are banned from transferring sensitive data to third parties without affirmative consent from the individual to whom the data pertains.[78] Thus, assuming that the bill is adopted and signed into law, if a covered entity is found to be transferring sensitive data to offshore entities without individuals' express consent, the Federal Trade Commission (FTC) could seek injunctive relief through an enforcement action. In such a case, the FTC would seek an order that halts the related data transfers. Such an order could be considered a restriction on data flows based on the USMCA cross-border data flows model.

Industry-favored digital trade rules may prevent effective enforcement of privacy legislation. These enforceability hurdles explain recent attention paid to digital trade negotiations by U.S. lawmakers. During the past two years, Representative Jan Schakowsky (D-IL-09) — one of the most important Democratic privacy advocates in Congress — has emerged as one of the first and most prominent congressional leaders advocating for policy space in the context of digital trade rules.[79] If governments do not retain the ability to regulate, or set conditions for, cross-border data transfers, they risk being unable to enforce their own laws. Provisions that force governments to allow the unconditional cross-border transfer of data will create deregulatory "data havens," which companies could use to evade data protection responsibilities.

77 California Legislature, Health Information, AB 352, introduced in Assembly January 31, 2023, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB352.

78 U.S. House, American Privacy Rights Act of 2024, HR 8818, 118th Congress, 2nd sess., introduced in House June 25, 2024, https://www.congress.gov/bill/118th-congress/house-bill/8818/text.

79 "Schakowsky, Lawmakers Reiterate Concern Over Big Tech Pushing Digital Trade Rules that Conflict with Biden Competition Agenda and Pending Legislation," Office of United States Congresswoman Jan Schakowsky, last modified April 24, 2023, https://schakowsky.house.gov/media/press-releases/schakowsky-lawmakers-reiterate-concern-over-big-tech-pushing-digital-trade.

DIGITAL TRADE RULES DO NOT SAFEGUARD DATA SECURITY POLICIES

The security of sensitive data and algorithms is another consideration that drives international data transfer regulation and domestic data storage requirements in many countries. Data security implicates people's personal security, as well as the economic security of individuals and businesses. In the United States in recent years, the data security debate has focused significantly on national security, which has also been the focus of some other countries' data security policies. South Korea demonstrates an interesting use case. South Korea's Land Survey Act prevents the unrestricted transfer of map data outside the country due to national security concerns. The government has offered to allow cross-border map data transfers, but only with the locations of sensitive infrastructure blurred out.[80]

At the EU level, a discussion on data sovereignty is taking place surrounding the European Cybersecurity Certification Scheme for Cloud Services (EUCS), proposed by the European Union Agency for Cyber Security (ENISA) in 2020 based on the EU Cybersecurity Act. Data sovereignty requirements were included in subsequent drafts after pressure from several member states, primarily France. These drafts required companies offering certain types of services with a need for the highest security standards to be immune from foreign law and process data solely within the EU. The certification scheme is still being heavily discussed. Although certification is voluntary based on the Cybersecurity Act, they could legally be made mandatory under an EU-wide cybersecurity instrument called the NIS2 Directive for certain entities by the European Commission or member states. Governments could also require such a certification in public procurement, making them de facto mandatory.[81]

The United States, too, has instituted domestic data storage requirements for sensitive defense-related data. Since 2015, the Defense Federal Acquisition Regulation Supplement requires cloud computing service providers to maintain all defense-related government data that is not physically located on the Department of Defense premises within U.S. territory, unless otherwise authorized by the authorizing official.[82] In October 2023, the Department of Defense, General Services Administration, and NASA proposed expanding this requirement to non-defense, high-impact federal information systems by amending the Federal Acquisition Regulation (FAR). This proposal — based on an executive order requiring agencies to standardize cybersecurity contractual requirements — is going through the rulemaking process.[83] The policy is flexible;

80 Julia Yoon, "South Korean Data Localization: Shaped by Conflict," University of Washington, Henry M. Jackson School of International Studies, last modified February 28, 2018, https://jsis.washington.edu/news/south-korean-data-localization-shaped-conflict/.
81 Lisa Peets, Marty Hansen, Mark Young, and Bart Szewczyk, "Implications of the EU Cybersecurity Scheme for Cloud Services," Inside Privacy, November 1, 2023, https://www.insideprivacy.com/cybersecurity-2/implications-of-the-eu-cybersecurity-scheme-for-cloud-services/.
82 U.S. Department of Defense, DFARS, Section 239.7602-2.
83 Federal Register, Federal Acquisition Regulation: Standardizing Cybersecurity Requirements for Unclassified Federal Information System.

it allows for cross-border data transfer with the approval of a relevant authorizing official.[84] However, even such a flexible policy linked to legitimate national security interests would run the risk of violating the extreme language forbidding government regulation of data.

Perhaps most importantly, these broad restrictions on data regulation, if agreed on at a plurilateral level, would prohibit the new restrictions on data brokers established by Congress in the Protecting Americans' Data from Foreign Adversaries Act of 2024. On April 24, 2024, President Biden signed into law a national security and foreign aid package which included the Protecting Americans' Data from Foreign Adversaries Act of 2024. This law, which the U.S. House of Representatives unanimously passed, prohibits data brokers from transferring U.S. residents' sensitive data to foreign adversaries.[85] The law explicitly forbids certain data transfers, which would violate the JSI cross-border data flows terms proposed by the U.S. government in 2019, from which support was withdrawn in 2023 consistent with new domestic policy.

The proposed constraints would also undermine President Biden's February 28, 2024, executive order on data security and its implementing regulation, which becomes effective on April 8, 2025. That order called for the Department of Justice to issue regulations to prohibit the transfer of bulk sensitive personal data and U.S. government data to countries of concern.[86] In January 2025, the Department of Justice issued its final rule implementing the order.[87] According to the new regulation, certain classes of highly sensitive transactions with countries of concern or entities linked to these countries are prohibited. This includes, for instance, data brokerage arrangements that give access to bulk sensitive personal data, including personal identifiers, precise geolocation data, biometrics, health data, and financial data. Some other transactions are restricted, unless they comply with predefined security to mitigate the risk of access to bulk U.S. sensitive personal data by malign actors. While this policy does not establish "generalized data localization requirements," trade pact rules — particularly in the context of the WTO — that could ban all conditions on cross-border data transfers would expose it to challenges at a trade agreement enforcement tribunal.

It is important to note that while the version of the JSI text most recently proposed by the countries leading those talks does not include terms regarding data transfers, it does include exceptions that would apply to the entire deal.[88] The text merely states that the corresponding security exceptions of the WTO GATT and GATS apply to this agreement. But the GATT and GATS security exceptions set forth limited grounds for when a country may be able to justify policies otherwise inconsistent with the rules. Basically, the exceptions can only potentially defend security policies related to fissionable materials

84 U.S. Department of Defense, DFARS, Section 239.7602-2.
85 Angelika Munger, "House Passed New Bill to Prohibit Data Brokers from Transferring Sensitive Data to Foreign Adversaries," The National Law Review, March 21, 2024, https://www.natlawreview.com/article/house-passed-new-bill-prohibit-data-brokers-transfering-sensitive-data-foreign.
86 "Executive Order 14117."
87 Federal Register, Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, A Rule by the Justice Department, January 8, 2025, https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern#sectno-reference-202.301.
88 World Trade Organization, "Joint Statement Initiative on Electronic Commerce," INF/ECOM/87, July 26, 2024, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/87.pdf&Open=True.

or military supplies trade, or in cases of war or "other emergency in international relations."

Countries have limited abilities to successfully use the WTO security exceptions to defend domestic policies, given that WTO enforcement tribunals have interpreted the concept of "emergency in international relations" very narrowly. Indeed, WTO panels ruled against the United States on two occasions already with respect to U.S. attempts to use this security exception to defend various China-related trade policies.[89] These rulings made clear that the GATT/GATS security exception model is completely ineffective in a world of increasing geopolitical tensions. Namely, trade tribunals seem to have concluded that a country must be engaged in active military conflict with another nation or on the brink thereof to meet the "emergency in international relations" condition.

The security exception that the United States has included in its FTAs since the pact signed with Singapore in 2003 provides an example of a more effective approach, which could be applied to rules governing the regulation of data transfers. The U.S. FTA security exception language basically ensures that each country determines its essential security interests and whether the policies it adopts are necessary to protect such interests.[90] More recent U.S. agreements, such as those with Peru or Korea, even include a footnote stating that the tribunal or panel adjudicating such a complaint shall find that the exception applies if the security exception is invoked in the dispute settlement procedure of the FTA. The digital trade rules in the Regional Comprehensive Economic Partnership, an initiative led by the Association of Southeast Asian Nations (ASEAN), include such a self-judging security exception, which allows countries to determine the content of their essential security interests. As with the U.S. FTA security exception language in recent agreements, a country's self-assessment of its security interests is not open to challenge by other countries.[91]

If trade agreements contain rules on cross-border data transfers, given that countries will regulate data issues for national security purposes, such pacts will require self-judging security exemptions such that countries retain sovereignty over data-related security decisions. Yet the absolute need for such an expansive security exception raises a key question: Is it really wise to commit to unfettered data transfers, particularly among geopolitical rivals, in a world where security-related regulation in the digital sphere grows more and more important every day?

89 World Trade Organization, "United States – Certain Measures on Steel and Aluminium Products: Report of the Panel," WT/DS544/R, December 9, 2022, https://www.worldtradelaw.net/document.php?id=reports/wtopanels/us-steelaluminum(panel)(china).pdf; World Trade Organization, "United States – Origin Marking Requirement: Report of the Panel," WT/DS597/R, December 21, 2022, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/DS/597R.pdf&Open=True.

90 "U.S.-Singapore Free Trade Agreement," conclusion date: May 6, 2003, Art. 21.2(b), https://ustr.gov/sites/default/files/uploads/agreements/fta/singapore/asset_upload_file708_4036.pdf#page=233.

91 "Regional Comprehensive Economic Partnership (RCEP)," conclusion date: November 15, 2020, Art. 12.14(3)(b), http://fta.mofcom.gov.cn/rcep/rceppdf/d12z_en.pdf#page=9.

DIGITAL TRADE INTRUSIONS IN GOVERNMENTS' ABILITIES TO GOVERN DATA TRANSFERS COULD AFFECT TAX POLICY

As Big Tech corporations continue to dominate the global economy, these firms' monopoly power has led to concerns about adequate taxation. The digitalization of the economy leads to two interconnected taxation problems:

Base erosion and profit shifting: The dominance of multinational companies can erode local tax bases. This issue is pervasive across economic sectors, but the damage is especially acute when it comes to digital services that can be delivered from anywhere in the world. When governments seek to tax profit, companies can report profit in low-tax jurisdictions to minimize the taxes they pay globally. The OECD estimates that, globally, $240 billion is lost annually due to tax avoidance by multinational companies.[92]

Taxation of intangibles and the use of data: Value drivers in the digital economy can often be intangible and do not require a physical presence in most jurisdictions where digital companies operate. Data is, of course, a key input of the value generated by digital companies (explaining much of their advocacy for unrestricted cross-border data flows). Traditional tax systems are unable to appropriately tax economic activities with these characteristics. Moreover, many scholars, governments, and international organizations now view data as an economic resource and believe that some of its value belongs to the populations from which it is being generated.[93]

To overcome these challenges, experts and policymakers have considered a number of proposals for taxing the collection or sale of certain data, including in the United States. In Washington state in 2017, for instance, State Rep. Norma Smith proposed HB 1904, which would impose a business and occupation tax of 3.3% on the sale of personal data related to residents of Washington state.[94] Washington's House Committee on Technology and Economic Development recommended passage of the bill in 2017. However, after industry lobbyists testified against it,[95] the proposal was not adopted by the full legislature.[96] There have been multiple data taxation proposals in

92 "Base Erosion and Profit Shifting (BEPS)," Organisation for Economic Co-operation and Development, accessed November 1, 2024, https://www.oecd.org/tax/beps/.

93 Satyanarayana Jeedigunta, Purushottam Kaushik, Nadia Hewett, and Arushi Goel, "Towards a Data Economy: An Enabling Framework," World Economic Forum White Paper (2021), https://www.weforum.org/publications/towards-a-data-economy-an-enabling-framework/; Stuart Mills, "Who Owns the Future? Data Trusts, Data Commons, and the Future of Data Ownership," SSRN Working Paper (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3437936; "Capitalizing on the Data Economy," MIT Technology Review Insights, last modified November 16, 2021, hittps://www.technologyreview.com/2021/11/16/1040036/capitalizing-on-the-data-economy/.

94 Washington State Legislature, Relating to the Sale and Taxation of Washingtonians' Personal Information and Related Data, HB 1904, introduced in House February 2, 2017, https://apps.leg.wa.gov/billsummary/?BillNumber=1904&Year=2017&Initiative=false.

95 John Stang, "Proposed State Tax on Sale of Personal Data Faces a Fight from Business Groups," GeekWire, March 11, 2017, https://www.geekwire.com/2017/proposed-state-tax-sale-personal-data-faces-fight-business-groups/.

96 Omri Marian, "Taxing Data," BYU Law Review 47, no. 2 (2022), https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=3349&context=lawreview; Washington State Legislature, HB 1904.

New York since at least 2019.[97] A similar "data dividend" proposal has been made by California Governor Gavin Newsom.[98]

Policies taxing the sale, transfer, or processing of data could be challenged under the most invasive trade agreement formulations banning international data-transfer regulation. As mentioned before, the USMCA model for cross-border data flows obligations bans any kind of prohibition or restriction on the international movement of data. It is important to note that the term "restriction" has been broadly interpreted by trade law international adjudicating bodies. For instance, the WTO Appellate Body defined restriction as "'[a] thing which restricts someone or something, a limitation on action, a limiting condition or regulation', and thus refers generally to something that has a limiting effect."[99] The broad interpretation of restrictions under international trade law means that the USMCA obligation to preserve free data transfers could encompass a wide range of policies that might merely affect or condition — but not necessarily ban — the movement of data across borders.

For instance, if Washington state enacted a tax on the sale of personal data and this tax discouraged some firms from selling data to overseas customers, a business or a group of businesses located in a USMCA country could claim that the personal data sales tax is an illegal restriction on the cross-border movement of data. If said business or group of businesses successfully recruited their government to launch a dispute against this policy, it would be hard to argue that a sales tax that could indeed reduce the number of data transfers — and in a way might be intended to do exactly that — is not a restriction on the movement of data. This means that the United States would have to rely on the deficient exception language included in the USMCA (see Box 3) to try to defend this policy from a trade challenge; if lost, the challenge could result in trade sanctions until the policy was eliminated.

Such conflicts with prospective measures that, even if not yet adopted, could be part of future data governance frameworks highlight the dangers of adopting broad obligations limiting the regulation of international data transfers.

97 New York State Senate, Creates an Excise Tax on the Collection of Consumer Data by Commercial Data Collectors, SB 4959, introduced in Senate February 19, 2021, https://www.nysenate.gov/legislation/bills/2021/S4959; New York State Senate, Establishes the Office of Consumer Data Protection and Imposes a Tax on Data Controllers and Data Processors, SB 6727, introduced in Senate May 13, 2021, https://www.nysenate.gov/legislation/bills/2021/S6727; New York Senate, Relates to a Tax on Gross Income Upon Every Corporation which Derives Income from the Data Individuals of this State Share with Such Corporations, SB 6102, introduced in Senate May 16, 2019, https://www.nysenate.gov/legislation/bills/2019/S6102.

98 Jasmine Ulloa, "Newsom Wants Companies Collecting Personal Data to Share the Wealth with Californians," Los Angeles Times, May 5, 2019, https://www.latimes.com/politics/la-pol-ca-gavin-newsom-california-data-dividend-20190505-story.html.

99 World Trade Organization, "China – Measures Related to the Exportation of Various Raw Materials: Reports of the Appellate Body," WT/DS394/AB/R, WT/DS395/AB/R, WT/DS398/AB/R, January 30, 2012, para. 319, https://www.wto.org/english/tratop_e/dispu_e/394_395_398abr_e.pdf.

DIGITAL TRADE RULES COULD UNDERMINE AI POLICY AND DATA REGULATION BEYOND PERSONAL DATA PROTECTION

The explosive growth in AI technology in recent years has brought back into focus the importance of personal and non-personal data as a resource. While traditionally personal data protection has been the focus of regulation, recently, policymakers have started to take an interest in non-personal data. Non-personal data is information that is not related to an identified or identifiable individual. AI models are trained on large amounts of both personal and non-personal data. The quality and quantity of such training data is a key determinant of an AI model's capabilities.

Policymakers are concerned about the concentration of data resources in a small number of companies, which could result in today's most dominant digital platforms also developing monopolies in AI products and services.[100] Such concerns apply to countries as well. If a country is able to freely collect data from across the world, it can develop more competitive and capable AI models. Such capabilities can allow such a country to dominate global AI markets in addition to all other economic activities affected by AI. Notably, President Biden's executive order on sensitive personal and U.S. government data also mentions the strategic advantage that these "countries of concern" can derive from unrestricted cross-border data transfers.[101]

These concerns are expressed not only through the data sale and collection tax proposals described above, but also policies establishing data-sharing mandates. For instance, in the health sector, policies on data sharing and interoperability implemented by the Biden administration through the Department of Health and Human Services require the sharing of data with different stakeholders, including community providers and the public.[102] California has a statewide health data-sharing agreement, which requires that hospitals, insurers, and clinical laboratories share information on treatment, payment, or health care operations through a set of standards called the Data Exchange Framework.[103] Scholars have suggested that mandatory data sharing can also be a way to break up monopolies, such as in online search.[104] The canonical example of mandatory data-sharing is the system of open banking in the European Union created by the revised Payment Services

100 "Generative AI Raises Competition Concerns," Technology Blog, Federal Trade Commission, last modified June 29, 2023, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns.

101 "Executive Order 14117."

102 "New Data-Sharing and Interoperability Mandates Create New Challenges," Avalere, last modified April 28, 2021, https://avalere.com/insights/new-data-sharing-and-interoperability-mandates-create-new-challenges.

103 Adam Hepworth, "California: Health Care Providers Must Join Statewide Data Sharing Agreement by 2024," The National Law Review, July 26, 2022, https://www.natlawreview.com/article/california-health-care-providers-must-join-statewide-data-sharing-agreement-2024.

104 Bertin Martens, "What Should Be Done About Google's Quasi-Monopoly in Search? Mandatory Data Sharing versus AI-Driven Technological Competition," Bruegel, last modified July 6, 2023, https://www.bruegel.org/working-paper/what-should-be-done-about-googles-quasi-monopoly-search-mandatory-data-sharing-versus; Andrea Vigorito, "Government Access to Privately-Held Data: Business-to-Government Data Sharing," European Journal of Comparative Law and Governance 9, no. 3: 237–258, https://doi.org/10.1163/22134514-bja10030; Inge Graef and Jens Prufer, "Mandated Data Sharing Is a Necessity in Specific Sectors," Economisch Statistische Berichten 103, no. 4763 (2018): 298–301, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3206685.

Directive (PSD-2) in 2018.[105] PSD-2 mandates the sharing of payments data through customer requests with other providers in the market, allowing new financial market players like payment apps to compete with large banks. The European Union's 2023 Data Act also has rules for mandatory non-personal data-sharing from private actors to the public sector and between private actors.[106] The Digital Services Act and Digital Markets Act also have rules on data-sharing and access, which apply for very large online platforms and gatekeepers, respectively.[107] These legislative efforts are a key pillar of the EU's strategy to create common European data spaces, which are ecosystems built by data infrastructures and governance frameworks and can be used by domestic and third-country businesses alike with the goal of reducing data asymmetries.[108]

In the case of data-sharing mandates, industry actors might attempt to leverage broad data flows obligations to challenge policies that limit international data transfers. As a reminder, the USMCA model of cross-border data flows obligations prohibits restrictions on the movement of data across borders. In trade law, restriction is traditionally interpreted as anything that has a limiting effect. If businesses can claim — and successfully convince their governments — that data-sharing mandates are so onerous that they limit their abilities to conduct business operations in the jurisdiction with such policies, they could argue that this measure constitutes a restriction on the movement on data, which would be prohibited under expansive cross-border data flows rules. As a matter of fact, the U.S. Chamber of Commerce has made precisely this claim against the EU Data Act.[109] Right now, there are no unrestricted data-transfer obligations between the United States and the EU. However, if language such as that included in USMCA were to be included in an instrument like the JSI on E-Commerce, these EU policies could be left vulnerable to corporate attacks.

105 "The Revised Payment Services Directive (PSD2) and the Transition to Stronger Payments Security," European Central Bank, last modified March 2018, https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html.

106 "Data Act," European Commission, accessed March 21, 2024, https://digital-strategy.ec.europa.eu/en/policies/data-act.

107 Luca Belli, "Data Sharing and the Delegated Act of Europe's DSA," Tech Policy Press, December 11, 2024, https://www.techpolicy.press/data-sharing-and-the-delegated-act-of-europes-dsa/; "Data Sharing Obligations Under the DMA: Challenges and Opportunities," Centre for Information Policy Leadership, last modified May 2024, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/data_sharing_obligations_under_the_dma_-_challenges_and_opportunities_-_may24.pdf.

108 "Commission Staff Working Document on Common European Data Spaces," European Commission, last modified January 24, 2024, https://digital-strategy.ec.europa.eu/en/library/second-staff-working-document-data-spaces.

109 Jordan Heiber and Garrett Workman, "The EU Data Act: A Misguided Policy: Forced Data Sharing & Restricted Data Flows Would Harm Economy, Undermine Cooperation," U.S. Chamber of Commerce, last modified March 2, 2023, https://www.uschamber.com/international/the-eu-data-act-a-misguided-policy.

Examples of international data-transfer limitations regarding non-personal data

Worldwide, some laws and proposals recognize that the unrestricted cross-border transfer of even non-personal data can carry risks. In the EU, these include the Data Governance Act and the Data Act.[110] The 2022 Data Governance Act provides for the possibility of limiting the cross-border transfer, where appropriate, of some non-personal data held by public-sector bodies and other organizations in order to protect trade secrets and intellectual property rights and to protect EU citizens against de-anonymization of non-personal data.[111] The 2023 Data Act, which covers commercial entities, also limits the cross-border transfer of non-personal data in certain situations. Article 32 of the Data Act, for instance, is concerned with preventing "international governmental access to or transfer of non-personal data held in the Union where such access or transfer would create a conflict with Union law or the national law of the relevant Member State."

Trade associations representing tech interests have claimed since these acts were first proposed that "unjustified data transfer restrictions" could be at odds with the EU's trade commitments.[112] Most of the limitations mentioned in this box are not directly connected to the protection of personal data. As such, personal data protection exceptions, such as the one proposed by the EU at the WTO, would not prevent challenges against these policies. In these cases, the EU would have to rely on the so-called "public policy" exception language, which is largely ineffective (see Box 3), to defend against a challenge to its Data Act or Data Governance Act.

110 Kristof Van Quathem and Anna Oberschelp de Meneses, "EU Rules Restricting the International Transfers of Non-Personal Data," Inside Privacy, last modified February 1, 2024, https://www.insideprivacy.com/health-privacy/eu-rules-restricting-the-international-transfers-of-non-personal-data/.

111 Regulation 2022/868 of the European Parliament and of the Council, On European Data Governance and Amending Regulation 2018/1724 (Data Governance Act), Official Journal of the European Union (2022), Recitals 20 and 24, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868.

112 "The European Commission Proposes New EU Data Sharing Rules, Expands Restrictions for International Transfers of Certain Data," Computer & Communications Industry Association, last modified November 25, 2020, https://ccianet.org/news/2020/11/the-european-commission-proposes-new-eu-data-sharing-rules-expands-restrictions-for-international-transfers-of-certain-data/.

Another illustrative case in relation to AI regulation is the FTC's power of disgorgement. If the FTC finds that an algorithm or model was trained on improperly obtained data, it can require that the data and the algorithm or model be deleted.[113] The FTC has used this regulatory power in the case of Cambridge Analytica, among other contexts.[114] In 2021, the FTC determined that Everbaum, a photo-storage business, had illegally developed facial recognition models based on customer data. The FTC's power of disgorgement allowed it to order Everbaum to delete the illegally held data and illegally developed models.[115]

This enforcement authority, which will be increasingly important as data disputes plague AI development, could be challenged under expansive rules banning data-transfer restrictions. For instance, if a foreign firm could claim that an order to disgorge ill-obtained data is a restriction on the flow of information it needs to conduct business, such enforcement action could be challenged under a trade agreement that replicates the USMCA model for cross-border data flows obligations.

This is not a far-fetched notion. For years, European data privacy authorities have been trying to sanction U.S.-based company Clearview due to GDPR violations committed while it built its facial recognition software. Among other enforcement actions, the French, Dutch, Italian, and Greek data protection authorities have imposed multimillion-euro penalties on Clearview; have ordered the company not to collect and process data on individuals located in these countries without a proper legal basis; and have ordered the company to delete data pertaining to individuals whose information it had processed unlawfully. So far, Clearview has refused to comply, claiming that it does not have a place of business nor any customers in the EU.[116] It is entirely likely that, were a rule banning data-flow regulation between the United States and the EU in effect, Clearview would argue that the French regulators' orders are illegal barriers to trade. Similar issues could arise with innumerable tech companies wishing to avoid compliance with the law.

The popularization of generative AI has profoundly impacted the tech policy debate worldwide. It is virtually impossible to anticipate what AI regulatory model will prevail. Yet training data is one of the key building blocks of these technologies, and rules on how it is collected, stored, used, and transferred are likely to be a fundamental component of the AI regulatory ecosystem. Trade rules banning data-transfer regulation could crucially undercut the implementation of AI policies that establish guardrails and guarantees in the development and deployment of these technologies.

113 Tonya Riley, "The FTC's Biggest AI Enforcement Tool? Forcing Companies to Delete Their Algorithms," CyberScoop, July 5, 2023, https://cyberscoop.com/ftc-algorithm-disgorgement-ai-regulation/.
114 Riley, "The FTC's Biggest AI Enforcement Tool?"
115 Heather Federman, "Tainted Fruit: Disgorgement of Data from the FTC and Beyond," International Association of Privacy Professionals, last modified April 27, 2021, https://iapp.org/news/a/tainted-fruit-disgorgement-of-data-from-the-ftc-and-beyond/.
116 Natasha Lomas, "Clearview Fined Again in France for Failing to Comply with Privacy Orders," TechCrunch, May 10, 2023, https://techcrunch.com/2023/05/10/clearview-ai-another-cnil-gspr-fine/.

CONCLUSION

Until recently, most discussions about the risks of imposing rules on data transfers and storage regulations have focused primarily on their impact on personal data protection. This paper explains why these risks are significant, but it also argues that such digital trade rules could have far-reaching consequences in the emerging data governance landscape beyond personal data protection. The data economy has only exploded in the last 20 years, and experts, policymakers, and regulators are just beginning to understand what policies are needed to ensure that these critical technologies and production processes benefit people and foster competitive markets, among other public interest goals. Given this context, policymakers and trade negotiators must exercise caution when considering binding commitments in commercial agreements that could preempt policy solutions in this developing field.

APPENDIX

The charts below compare three distinct models of international data flows commitments found in existing trade agreements with digital trade or e-commerce terms. The columns, from left to right, include the terms of the 2019 USMCA, the 2021 Mercosur E-Commerce Agreement, and the provisions from the 2022 EU-New Zealand trade agreement.

Regarding data flows and location of computing facilities language in digital trade agreements, there are two levels of focus: (i) the "obligation" with which countries are agreeing to conform their domestic law; and (ii) the exceptions to that obligation, which would safeguard certain policies from trade challenges.

The chart below shows side-by-side the obligations agreed to by the parties to these three agreements.

USMCA	Mercosur	EU-New Zealand
Obligations		
Art. 19.11: Cross-Border Transfer of Information by Electronic Means "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." **Art. 19.12: Location of Computing Facilities** "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."	**Art. 7: Cross-Border Transfer of Information by Electronic Means** "Each Party shall allow the cross-border transfer of information by electronic means when this activity is for the conduct of the business activity of a person of a Party. For greater clarity, this paragraph is subject to compliance with Article 6.7." **Art. 8: Location of Computing Facilities** "A Party shall not require a person of a Party to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."	**Art. 12.4: Cross-Border Data Flows** "(...) a Party shall not restrict cross-border data flows taking place between the Parties in the context of activity that is within the scope of this Chapter, by: (a) requiring the use of computing facilities or network elements in its territory for data processing, including by requiring the use of computing facilities or network elements that are certified or approved in the territory of the Party; (b) requiring the localisation of data in its territory; (c) prohibiting storage or processing of data in the territory of the other Party; or (d) making the cross-border transfer of data contingent upon the use of computing facilities or network elements in its territory or upon localisation requirements in its territory."

A thorough comparison reveals key differences in the scope of the commitments assumed by the parties of each agreement:

While the USMCA broadly forbids any kind of government restriction on the cross-border transfer of data, the Mercosur model includes a positive obligation to "allow the cross-border transfer of information by electronic means." The term "restriction" has been broadly interpreted by trade law international adjudicating bodies, which have deemed that anything that has a limiting effect could be a restriction.[117] This means that, by prohibiting any restriction on the cross-border movement of information, the USMCA model imposes a broad, open-ended negative obligation on state parties with far-reaching consequences for data regulation. Conversely, Mercosur countries did not relinquish their right to regulate or even limit data transfers in specific circumstances; allowing the movement of data does not mean that countries cannot adopt conditions to ensure that said movement respects privacy, data security, etc.

Notably, the EU-New Zealand deal, which incorporates the EU horizontal rules on privacy and cross-border data flows, does not include a broad obligation either to avoid restrictions or allow data flows, like the USMCA and the Mercosur model do. The EU model explicitly bans the use of tools of forced localization between the signing countries while leaving room for international data-transfer regulation.

Regarding the location of computing facilities rules in USMCA and the Mercosur deal, these terms are functional equivalents to the specific prohibitions included in the EU cross-border data flows language. This corroborates that the cross-border data flows obligations in USMCA and Mercosur go beyond prohibiting data localization measures.

Another notable difference between the USMCA and Mercosur model relative to the EU position is that the first two establish rights for businesses, instead of only setting parameters for government action. One of the main consequences of this difference is that the USMCA and the Mercosur rules guarantee rights for data to flow to any country as long as it is for the conduct of business by an investor or service supplier of a signatory of the agreement. In contrast, the EU construct guarantees free flows between signatory countries only.

When it comes to the specific exceptions that have been included in these provisions, there are important differences as well. The chart below shows side-by-side the exceptions language that is supposed to provide policy space for countries to regulate in the public interest.

117 WTO, "China – Measures Related to the Exportation of Various Raw Materials," para. 319.

USMCA	Mercosur	EU-New Zealand
Exceptions		
Art. 19.11: Cross-Border Transfer of Information by Electronic Means "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."[118]	**Art. 7: Cross-Border Transfer of Information by Electronic Means and Art. 8: Location of Computing Facilities** "Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade."	**Art. 12.4: Cross-Border Data Flows** "For greater certainty, the Parties understand that nothing in this Article prevents the Parties from adopting or maintaining measures in accordance with Article 25.1 (General Exceptions) to achieve the public policy objectives referred to therein, which, for the purposes of this Article, shall be interpreted, where relevant, in a manner that takes into account the evolutionary nature of the digital technologies. The preceding sentence does not affect the application of other exceptions in this Agreement to this Article." "Each Party may adopt or maintain measures it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this Agreement shall affect the protection of personal data and privacy afforded by the Parties' respective measures."

118 This exception is only applicable to the cross-border data flows obligation. The USMCA did not include a specific exception for the location of computing facilities provision.

The most notable differences between these models are:

» First, in its trade pacts based on the horizontal provisions, such as with New Zealand, the EU accompanies the cross-border data flows obligation with a largely self-judging privacy exception. A self-judging exception is by far the strongest format and is used by the United States for its FTA security exceptions. Such an exception leaves no room for a trade tribunal to second-guess a government. In this case, in the event of a challenge, a defending government does not have to demonstrate that its policy is necessary, essential, or required to protect personal data and privacy. As long as the policy is reasonably connected to data privacy objectives, the exception should trump any challenge.

» The other exceptions in these agreements are inspired by the WTO GATT and GATS general exceptions language. As explained in Box 3, tribunals have made these exceptions largely ineffective by establishing thresholds skewed in favor of commercial interests and trade liberalization over other societal goals.

» It is noteworthy that the Mercosur exception does not include a proportionality requirement, such as the necessity test, which has been fatal for many public interest policies at the WTO.

AMERICAN ECONOMIC LIBERTIES PROJECT

rethink TRADE

The American Economic Liberties Project is a new, independent organization fighting against concentrated corporate power to realize economic liberty for all, in support of a secure, inclusive democratic society.

Rethink Trade was established to intensify analysis and advocacy regarding the myriad ways that today's trade agreements and policies must be altered to undo decades of corporate capture and to deliver on broad national interests.

economicliberties.us
@econliberties
info@economicliberties.us

rethinktrade.org
@rethinktrade
info@rethinktrade.org

Closing the Gap:

Evaluating Rapid Response Labor Mechanism Outcomes and Charting a Path Through the 2026 USMCA Review

REPORT

rethink TRADE
AMERICAN ECONOMIC LIBERTIES PROJECT

SEPTEMBER 2025

Daniel Rangel, Research Director, Rethink Trade

Lori Wallach, Director, Rethink Trade

The authors thank Abigail Milligan and Katelyn Hettinga for their extensive and invaluable research contribution to this report. This report benefitted from feedback and conversations with a great number of people, including Anna Canning, Elizabeth Echevarria Manrique, Luis Espinosa-Organista, Benjamin Davis, Patricia Juan Pineda, Desirée LeClercq, Paolo Marinaro, Sarah Newell, Susana Prieto Terrazas, Sandra Polaski, Gabriela Rosazza, and Jason Wade. Their perspectives, assistance, and feedback improved this work in important ways. Errors and omissions are the responsibility of the authors.

Table of Contents

Executive Summary

The Rapid Response Mechanism (RRM), created by the United States-Mexico-Canada Agreement (USMCA), is an unprecedented tool designed to enforce labor rights via trade agreements. For the first time, a trade deal allows complaints against specific facilities that deny workers freedom of association or collective bargaining and makes possible direct sanctions on companies. The RRM's record demonstrates that including enforceable labor standards in a trade agreement can deliver tangible gains for workers, such as reinstatements after retaliatory firings, new opportunities for independent unions to organize, and stronger contracts. However, this research finds that, in the latter years of the mechanism's first five in operation, these gains have diminished as employers developed ways to limit durable remediation, while structural design flaws and ambiguities created off-ramps to evade sanctions. The key lesson from the RRM's first five years is that facility-specific trade-labor enforcement tools can be highly effective, but it is essential to address systemic shortcomings to ensure these tools deliver more consistently on their promises.

The RRM's transformational approach was designed to address decades of wage suppression in Mexico under employer-dominated unions and sham collective bargaining agreements (CBAs). The systematic suppression of fundamental labor rights and independent unions, along with the resulting rock-bottom wages, incentivized corporations to relocate thousands of industrial facilities from the United States to Mexico under the 1994 North American Free Trade Agreement (NAFTA). By mid-2020, the U.S. government had certified more than one million American workers as having lost their jobs due to offshoring and import competition under NAFTA. During his first term, President Trump promised that his NAFTA renegotiation and USMCA would end job offshoring to Mexico and the NAFTA trade deficit.

In its first five years, the RRM has produced important results. It led to reinstatement of workers fired for union activity, expanded access to trainings on freedom of association, and supported new opportunities for independent unions. Between July 2020 and June 2025, the United States initiated 37 RRM cases targeting 36 facilities involving mining, call centers and air transport services, food, electronics, apparel, and, most notably, automotive sector manufacturing.

Tens of thousands of workers in facilities where RRM cases succeeded have made real gains. But the USMCA has not delivered on topline promises to end the race to the bottom in wages and labor conditions or balance regional trade. Wages in Mexico remain very low despite some gains. Workers in the

automotive and electronics manufacturing sectors still earn only $3 to $5 per hour, even as productivity approaches U.S. levels. Manufacturing wages in Mexico remain about 40% lower than in China.

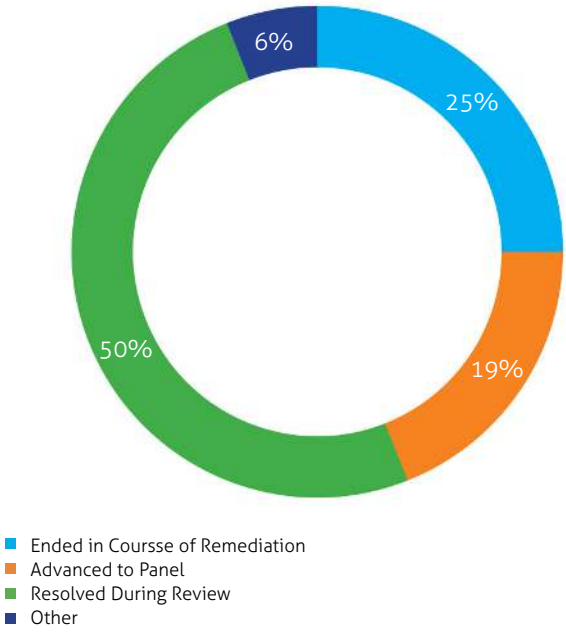
The mechanism's early implementation has highlighted areas where further progress is needed. Not enough cases have resulted in real penalties for employers violating labor rights to incentivize systemic, prophylactic changes, such as employers ending abuses against independent unions or improving pay and conditions. RRM remediation has sometimes taken the form of surface-level measures that, while accepted by governments, have not always resulted in durable improvements to workers' ability to organize and bargain collectively. Independent Mexican unions have made headway in certain facilities but still face challenges in securing contracts and meaningful wage gains after cases are closed. These patterns underscore the importance of using the mandatory 2026 USMCA review to refine the mechanism so that it can fulfill its long-term potential.

Key Findings:

1. The governments are "resolving" too many cases without securing long-term gains for workers.

By mid-2025, of 32 concluded cases initiated by the U.S. government concerning labor violations in Mexico, half were deemed "resolved during review," eight resulted in a formal Course of Remediation, and six advanced to panels—independent groups of three labor experts that determine whether violations occurred and whether they were remedied. The USMCA text does not clearly outline the consequences of cases being "resolved during review." The increasing tendency to close cases without a Course of Remediation or panel action calls into question whether this approach genuinely tackles union-busting practices or holds companies accountable through a clear record of denial-of-rights violations.

Pre-Panel Outcomes of known RRM Cases



2. Remediation has been real, but it is often standardized and insufficient in some cases.

Common remedies agreed by governments to end cases without panel activation include neutrality statements, worker reinstatements, and freedom of association (FOA) trainings. These measures are important steps, particularly the reinstatement of workers fired for their union activities or preferences. However, commitments to grant union access to facilities or recognize and bargain with petitioner unions have been less frequent. Strengthening remedies to prioritize actions that enable independent unions to organize and bargain collectively would help advance the core objectives of the RRM.

Top 10 Most Common Remediation Actions Achieved through the RRM

Common Remedial Actions	Total Number of Cases
Neutrality Statement and/or Zero-Tolerance Policy	26
Mexico-Provided FOA Training	24
Facility-Provided FOA Training	19
Worker Reinstatement and/or Backpay	19
Anonymous Hotline to Report Violations	14
Severance Payments	7
Union Access to Facility	7
Proper Management of Union Dues	6
CBA Distribution	5
Recognizing and Engaging in Bargaining with Petitioner Union	5

3. Progress has been made on freedom of association, but there is less movement on collective bargaining.

Twelve workplaces out of 32 concluded RRM cases saw workers gain new union representation and/or contracts, but a larger share of RRM cases did not produce such results. Early RRM cases were notably successful in delivering durable gains for workers. Later cases suggest that corporations have developed strategies to persuade authorities that limited actions amount to sufficient remediation without enabling workers to organize independent unions or negotiate strong collective bargaining agreements.

Union Representation and Collective Bargaining Outcomes of Concluded RRM Cases by Workplace

Workers gained new union representation and/or a new/ revised CBA	Workers only gained new union representation	RRM activity did not result in new union representation or a new/ revised CBA
1. General Motors (2021)	1. Manufacturas VU (2022)	1. Draxton (2023)
2. Tridonex (2021)	2. Unique Fabricating (2023)	2. Grupo México – San Martín mine (2023)
3. Panasonic (2022)		3. Grupo Yazaki (2023)
4. Teksid Hierro (2022)		4. Asiaway Automotive Components (2023)
5. Goodyear (2023)		5. Tecnología Modificada – Caterpillar (2023)
6. INISA (2023)		6. Fujikura* (2023)
7. Aerotransportes MAS de Carga (2023)		7. Atento Servicios (2024)
8. Teklas (2023)		8. RV Fresh Foods* (2024)
9. Autoliv (2023)		9. Servicios Industriales González (2024)
10. Minera Tizapa (2024)		10. Volkswagen* (2024)
11. Odisa (2024)		11. Impro (2024)
12. Modern Metal Alloys (2025)		12. Vidrio Decorativo Occidental (2024)
		13. Aludyne Automotive (2025)
		14. Superior Industries (2025)

The fact that half of all concluded RRM cases have not resulted in new union representation and/or a new or revised contract raises questions about the effectiveness of the mechanism to fulfill its ultimate objectives. The cases marked with an asterisk in the table are those in which securing new union representation or a new or improved collective bargaining agreement was likely not the petitioners' ultimate goal when filing the complaint.

4. Secrecy about why petitions are rejected or even how many are filed chills use of the RRM and hinders accountability.

There is no public information on the total number of petitions filed under the RRM, nor any transparency about the reasons some were rejected. Through a Freedom of Information Act (FOIA) request, we discovered that 56 petitions were filed during the first five years of the RRM, although one was later withdrawn. The U.S. government initiated action on 38 cases: 36 resulting from petitions and two self-initiated. But there is limited public information about why 19 petitions were rejected or otherwise did not trigger activation of the mechanism. The lack of transparency that has marked the RRM's initial years is a key area requiring improvement.

Summary of Recommendations for the 2026 USMCA Review:

Based on the findings in this report, we recommend a set of quick targeted adjustments and broader systemic improvements:

Targeted Adjustments:

1. Shorten the respondent Party's period for internal review: The respondent Party's 45-day internal review period should be shortened to 30 days, matching the complainant Party's timeline. While the U.S. government has demonstrated that such investigations can be completed within this shorter timeframe, Mexico's greater access to facilities and investigative tools makes a longer period unnecessary. More importantly, the current 45-day window often results in cases being superficially "resolved during review," with companies offering quick fixes that fail to address deeper violations of workers' rights. A 30-day limit would push for more substantive evaluations and reduce incentives for shallow remediation.

2. Extend or modify the Interagency Labor Committee's deadline to determine whether to invoke a panel: Congress should extend or modify the 60-day deadline imposed on the Interagency Labor Committee to decide whether to request a panel after invoking the RRM. Under current rules, the U.S. government has only 15 days following Mexico's 45-day internal review to make this determination, which can lead to premature closure of cases based on short-term or superficial remedies. Extending the deadline by 15 to 45 days—or allowing extensions when necessary—would provide sufficient time to assess whether commitments are being effectively implemented and ensure decisions reflect lasting improvements in workers' rights.

3. Require Parties to consult with stakeholders—especially petitioners—when developing remediation actions, and disclose investigation findings while safeguarding witness workers: Including petitioners in the Course of Remediation process would help ensure that remedies address ongoing violations, while sharing investigation outcomes in writing would strengthen accountability and improve the RRM's effectiveness.

4. Clarify that a "Resolved During Review" outcome counts as a Denial of Rights Determination: The mechanism is designed around escalating penalties, making it critical that corporations involved in violations face lasting consequences and an increased risk of future cases. The growing trend of categorizing outcomes as "resolved during review" raises concerns that governments and companies may use this designation to avoid a formal "first strike." Explicitly stating in the USMCA text that such cases qualify as Denial of Rights Determinations would strengthen deterrence and preserve the integrity of the penalty system established in Article 31-A.10.

5. Clarify that administrative and judicial authorities' actions can constitute a Denial of Rights under the RRM: The agreement does not require attributing violations solely to companies or governments, which is critical since employers often rely on protection unions or local authorities to obstruct workers' organizing and bargaining efforts. However, in practice, there has been reluctance to address violations involving administrative or judicial misconduct through the RRM. To reaffirm the Parties' intent, the USMCA text should be clarified to explicitly include such actions within the scope of the mechanism.

Systemic Improvements:

1. Add a substantive obligation requiring all USMCA Parties to ensure employers bargain in good faith: While the RRM has been effective in addressing freedom of association violations, remediation related to collective bargaining has been rare, in part because Mexican labor law does not explicitly require employers to negotiate in good faith. The result is that domestic enforcement often focuses on compliance with strike procedures rather than employers' bargaining conduct. To strengthen workers' ability to secure union contracts, the USMCA should include a clear obligation for all Parties to impose a duty to bargain in good faith, with a commitment for Mexico to amend its Federal Labor Law accordingly.

2. Require Mexico's Federal Center for Labor Conciliation and Registration to have sanctioning authority: While the RRM has advanced labor rights enforcement, it cannot address all violations. Amending the USMCA to require that Mexican law grant the Federal Center sanctioning authority—an initiative already approved by the lower house of Congress but stalled in the Senate—would bolster enforcement and extend protections nationwide.

3. Isolate fact-finding aspects of the RRM process and make it equally applicable to all USMCA Parties: Currently, governments must both investigate petitions and—in the case of Mexico—defend companies accused of labor rights violations, a conflict that undermines credibility. The process also lacks transparency, with neither petitioners nor companies having access to investigators' reports or evidence the other party submits. Establishing an independent body—potentially modeled

on precedents like the U.S.–Cambodia Textile Agreement or the Bangladesh Accord—would enhance impartiality, ensure stakeholders receive findings, and build trust in the system. Finally, extending the RRM to cover facilities in the United States and Canada would guarantee equal protection for workers across all Parties and prevent distortions in labor standards and competition.

The RRM offers a new model for labor enforcement via trade agreements. Unlike past trade pacts that relied on state-to-state disputes, the RRM provides facility-specific accountability. This represents a significant advancement in the trade and labor field and has already proven effective in addressing clear cases of rights violations. But for the RRM to deliver on its promises, critical improvements are necessary.

Introduction

Trade deals expose workers to competition from workplaces in other countries with different wage levels and labor conditions. Without strong labor rights and effective enforcement mechanisms, this competition can foster a race to the bottom in wages and working conditions at home and abroad.

The 1994 North American Free Trade Agreement (NAFTA) is a case in point. Since its implementation in 1994, unions lost bargaining power, jobs were offshored, and workers across the region experienced wage stagnation. NAFTA allowed multinational corporations to exploit the wage gap between U.S. and Mexican workers, offshoring hundreds of thousands of U.S. jobs to Mexico. The U.S. government certified 1,086,659 American workers as having lost their jobs due to offshoring and import competition from Mexico and Canada during NAFTA under the Trade Adjustment Assistance program, which is limited to workers who know to apply and meet specific standards.[1] NAFTA also impacted U.S. workers' collective bargaining power by suppressing unionization efforts using credible threats from employers to offshore production to Mexico.[2]

The 2020 United States-Mexico-Canada Agreement (USMCA), which replaced NAFTA after President Trump launched its renegotiation in his first term, includes stronger labor standards and a novel new system intended to address the race to the bottom in wages and work conditions that the original NAFTA generated. This innovative legal tool, called the Rapid Response Mechanism (RRM), complements the state-to-state dispute settlement mechanisms of older trade agreements. While state-to-state disputes emphasize government action, the RRM is novel because it empowers workers and unions to target specific facilities and companies that violate certain labor rights recognized by the USMCA—particularly those related to freedom of association and collective bargaining—by authorizing *trade sanctions directly against noncompliant companies*. No other trade agreement in the world has a similar labor-enforcement tool.

[1] This figure reflects the combined total of workers who received benefits under the NAFTA-specific Trade Adjustment Assistance (TAA) program, which operated from 1994 to 2001, and those certified under the general TAA program between 2002 and June 2020 for trade-related job losses caused by production shifts to or import competition from Mexico and Canada. Since narrow eligibility criteria and administrative hurdles affected TAA certifications, it is likely that the actual number of lost jobs is much higher. See U.S. Library of Congress, Congressional Research Service, Industry Trade Effects Related to NAFTA, RL31386 (2003), https://www.everycrsreport.com/files/20031030_RL31386_1000c2dc387396f020ca03a3da2da296f2a876c5.pdf and "Trade Adjustment Assistance Database," Public Citizen, accessed September 3, 2025, https://www.citizen.org/article/trade-adjustment-assistance-database/.

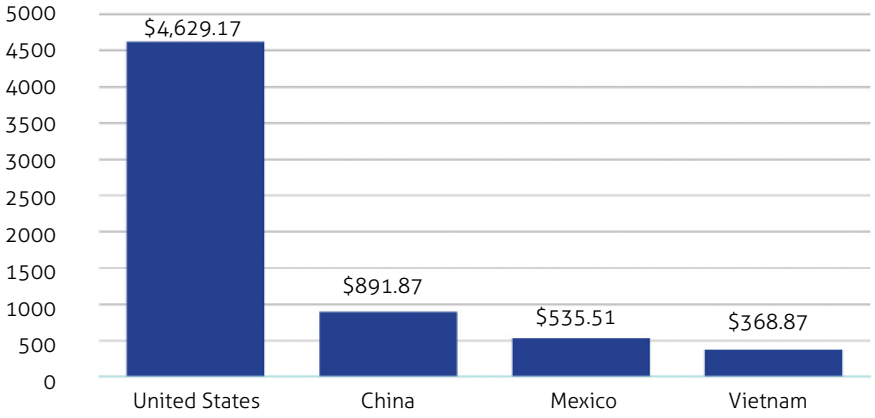
[2] An early study on NAFTA's impact on workers' right to organize in the United States found that at least 10% of U.S. union drives from 1993 to 1995 faced relocation threats supported by the passage of NAFTA. See Kate Bronfenbrenner, "Final Report: The Effects of Plant Closing or Threat of Plant Closing on the Right of Workers to Organize," Cornell University Digital Commons, North American Commission for Labor Cooperation, (1996), https://ecommons.cornell.edu/handle/1813/87617.

The USMCA also included specific commitments by Mexico to overhaul its labor relations system. Starting in the 1980s, company-dominated unionism became the prevailing model of collective bargaining in Mexico.[3] Under this system, unions act in employers' interests to suppress wage growth and block genuine collective bargaining by workers, often by signing collective bargaining agreements (CBAs) that lock in low wages and poor working conditions—frequently without workers' knowledge, let alone their consent. These agreements are locally known as 'protection contracts,' and the unions that operate this way are called 'protection unions.'[4] Mexican government labor institutions—comprising representatives of the government, employers, and unions—also created obstacles for workers by blocking their attempts to gain true union representation and by actively undermining independent unions. NAFTA reinforced corporations' ability to exploit this anti-worker system and pay suppressed wages as they relocated industrial facilities to Mexico.

This regime is one reason why manufacturing wages in Mexico are now roughly 40% lower than in China and only about 45% higher than in Vietnam, a country with considerably lower levels of development.

> Today, manufacturing wages in Mexico remain about 40% lower than in China.

Figure 1. 2024 Monthly Average Manufacturing Wage in USD – Nonsupervisory Employees



Sources: Author's elaboration based on official government data.[5]

[3] María Xelhuantzi López, *101 Años de Control Sindical en México (1918–2019): El Por Qué de los Bajos Salarios y la Desigualdad* (México: Cisnegro, Lectores de Alto Riesgo, 2019), ISBN 9786079320416, p. 25.
[4] Carlos de Buen Unna, "Collective Bargaining Agreements for Employer Protection ('Protection Contracts') in Mexico," *Friedrich Ebert Foundation*, (2011), https://www.academia.edu/7879996/Collective_Bargaining_Agreements_for_Employers_Protection_in_Mexico
[5] For U.S. wage data, see "Average Hourly Earnings of Production and Nonsupervisory Employees, Manufacturing," Federal Reserve Bank of St. Louis, accessed September 3, 2025, https://fred.stlouisfed.org/series/CES3000000008; for Chinese wage data, see "Average Annual Wages of Employed Persons in Enterprises Above the Designated Size by Sector and Position in 2024: Personnel Engaged in Production and Manufacturing – Manufacturing," National Bureau of Statistics in China, accessed September 3, 2025, https://www.stats.gov.cn/english/PressRelease/202505/t20250520_1959885.html; for conversion from yuan to USD, see "Yearly Average Currency Exchange Rates: China," U.S. Internal Revenue Service, accessed September 3, 2025, https://www.irs.gov/individuals/international-taxpayers/yearly-average-currency-exchange-rates; for "Mexican wage data, data extracted from the National Survey of Occupation and Employment (ENOE) for "Industrial Plant and Machinery Operators," INEGI, accessed September 12, 2025, https://en.www.inegi.org.mx/programas/enoe/15ymas/; for conversion from pesos to USD" U.S. Internal Revenue Service, accessed September 3, 2025, https://www.irs.gov/individuals/international-taxpayers/yearly-average-currency-exchange-rates; for Vietnam wage data, see "Monthly Average Income per Employee by Occupation: Plant and Machine Operators and Assemblers," National Statistics Office of Vietnam, accessed September 3, 2025, https://www.nso.gov.vn/en/px-web/; for conversion from dong to USD, see "Official Exchange Rate (LCU per US$, Period Average) – Viet Nam," World Bank, accessed September 3, 2025, https://data.worldbank.org/indicator/PA.NUS.FCRF?locations=VN.

Given this context, strengthening Mexico's labor institutions became a central focus of the NAFTA renegotiation. The 2018 midterm elections resulted in a Democratic majority in the U.S. House of Representatives. To gain Democratic votes, the Trump administration had to restart negotiations on its initial USMCA deal. The outcome was stronger labor standards, the creation of the RRM enforcement system, and a condition that the new agreement would not take effect until Mexico implemented and funded binding commitments to establish independent federal and state labor courts, conciliation centers to help resolve labor disputes, and democratic union practices—including personal, direct, secret-ballot voting for approving collective bargaining agreements and electing union leadership. In May 2019, Mexico enacted a sweeping labor reform to implement these changes, paving the way for the USMCA's entry into force the following year. The 2019 reform has transformed labor relations in Mexico and allowed the RRM to emerge as a useful tool for independent unions.

Yet despite five years of the RRM's operation, the implementation of Mexico's historic labor reform, and several increases in the federal minimum wage, wages in Mexico remain suppressed. Employer-aligned unions continue deeply entrenched, while independent unions have made only limited progress in narrowing the wage gap with the United States for the relatively small share of workers they represent. In 2024, unionized Mexican workers experienced their highest wage gain in two decades, yet real wages rose by just 2.2% year-over-year, highlighting the slow pace of meaningful improvement.[6] Mexican workers in highly productive sectors—such as automotive and electronics manufacturing—earn hourly wages of just $3 to $5, despite the convergence of productivity levels in U.S. and Mexican manufacturing. A 2019 study by the U.S. International Trade Commission underscores this point. According to the study, industry representatives have acknowledged that, for instance, productivity at Ford's Hermosillo stamping and assembly plant is comparable to that of a similar facility in the United States.[7] Yet workers at this plant earn only one-tenth of the wages negotiated by the United Auto Workers with the Big Three automakers in the United States in 2023. The wage gap poses an existential challenge to the long-term sustainability of the USMCA, one that could be mitigated in part by strategically leveraging the RRM.

From July 1, 2020 (the date when the USMCA entered into force), until June 30, 2025, there were 37 RRM cases initiated by the United States targeting labor rights abuses in 36 facilities. These cases have involved a range of economic sectors, including mining, call centers, apparel, air transportation, food manufacturing, and, most notably, automotive manufacturing. According to the U.S. Trade Representative (USTR), more than 42,000 workers have been positively affected by the RRM as of December 2024.[8]

[6] Gerardo Hernández, "Salarios Contractuales Alcanzaron en 2024 el Crecimiento Real Más Alto en Dos Décadas," *El Economista*, January 15, 2025, https://www.eleconomista.com.mx/capital-humano/2024-salarios-contractuales-alcanzaron-crecimiento-real-alto-dos-decadas-20250115-742129.html.

[7] United States International Trade Commission, *U.S.-Mexico-Canada Trade Agreement: Likely Impact on the U.S. Economy and on Specific Industry Sectors*, by Serge Shikher, Mihir Torsekar, Mitchell Semanik, and Peter Herman, Pub. No. 4889 (2019), at p. 217, n 611, https://www.usitc.gov/publications/332/pub4889.pdf.

[8] "United States Announces Successful Resolution of Rapid Response Labor Mechanism Matter at Odisa Facility," Office of the United States Trade Representative, December 20, 2024, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2024/december/united-states-announces-successful-resolution-rapid-response-labor-mechanism-matter-odisa-facility

The first mandatory joint review of the USMCA as required by the pact's text must be completed by July 2026. The review process is intended to ensure relevance and functionality of the agreement. As such, it presents an invaluable opportunity to conduct an in-depth analysis of the successes and potential shortcomings of the RRM so far to ensure that it supports a high-road labor model in North America.

This report contributes to that discussion by providing insight on the first five years of the RRM's operation. It begins with an overview of how the mechanism was designed by the USMCA Parties: the United States, Mexico, and Canada. This section will be followed by an analysis of the effectiveness of the mechanism in practice, looking at procedural outcomes; types of remediation; and the impact on union representation, bargaining, and wages in Mexico. Our analysis is focused on the cases that led the U.S. government to activate the mechanism. Through a Freedom of Information Act (FOIA) request, we discovered that 56 petitions were filed during the first five years of the RRM, although one was later withdrawn. However, there is limited public information about why 19 petitions were rejected or otherwise did not trigger the activation of the mechanism. The report will conclude with recommendations for the upcoming USMCA review to address gaps in the mechanism that hinder full protection of workers' rights and ensure that the RRM and USMCA can better deliver on their goals.

Facility-Specific Labor Enforcement:

How Was the USMCA's RRM Designed?

Before the USMCA, most trade agreements with labor provisions relied on state-to-state dispute settlement mechanisms to address potential violations of labor-related terms. Some older agreements, such as NAFTA, offered no recourse to dispute settlement for labor standards violations. Others, like the Dominican Republic–Central America Free Trade Agreement (CAFTA-DR), allowed challenges only when a country failed to enforce its own labor laws.[9] Several strict criteria had to be met for a trading partner to be held accountable for labor rights violations taking place in its territory, including "sustained or recurring" breaches of labor standards and proof by the complaining country that the violations affected trade or investment flows. The remedy available to a complaining country after proving these violations would not necessarily end up targeting the actors involved in the Denial of Rights. Remedies in these pacts involved a complaining country suspending concessions given through the trade agreement, usually in the form of retaliatory tariffs. That meant that the offending country could choose to absorb the sanctions as a cost of a low-road strategy of suppressing wages to attract foreign investment. Additionally, in cases where labor rights violations are committed by a specific company, retaliatory tariffs targeting an entire country or sector could potentially hurt both compliant and noncompliant actors.

The RRM addresses many of these design shortcomings. This tool creates a pathway to target and sanction *specific facilities* where workers' rights to freedom of association and collective bargaining are being undermined and to penalize companies abusing workers in more than one facility, including by denying access to export markets for goods or services produced in violation of the rules.

However, the RRM is an asymmetric tool. As a practical matter, it was added to the USMCA text via two annexes to the pact's Dispute

[9] Álvaro Santos, "The Lessons of TPP and the Future of Labor Chapters in Trade Agreements," in *Megaregulation Contested: Global Economic Ordering After TPP*, Law and Global Governance (Oxford, 2019), p. 140–74, https://doi.org/10.1093/oso/9780198825296.003.0007.

Settlement chapter through a protocol negotiated in 2019. The language of the annexes ensures that Canada and the United States can separately initiate disputes against Mexico, but all Parties are virtually barred from bringing claims against either Canadian or U.S. facilities.[10]

In terms of scope, the United States-Mexico Facility-Specific RRM applies to facilities located in Mexico that export goods or provide services to the United States, or those that compete with U.S. goods or services sold in Mexico. The Canada-Mexico system has an equivalent scope. Specifically, the RRM is available for workers in the manufacturing, mining, and services sectors. It excludes agriculture, which is the only economic sector not covered by the mechanism. Public stakeholders, such as labor unions, non-governmental organizations (NGOs), affected workers, and other interested parties can file a petition when freedom of association and collective bargaining rights have been violated to request that the U.S. or Canadian governments activate the RRM. It is worth underscoring that although the USMCA Labor Chapter protects a broad range of labor rights, the RRM applies only to a subset of them: freedom of association and collective bargaining.

The RRM can be triggered by a public petition submitted to the Office of Trade and Labor Affairs of the U.S. Department of Labor (OTLA), or the U.S. government can self-initiate the process. The petitions are reviewed by the Interagency Labor Committee for Monitoring and Enforcement (Interagency Labor Committee), a body created by the USMCA Implementation Act and co-chaired by the U.S. Trade Representative and the U.S. Secretary of Labor. Under the Canada-Mexico system, petitions may be submitted by Canadian nationals or enterprises to the Canadian National Administrative Office (NAO), or the mechanism can be self-initiated by the Canadian government.[11]

The RRM has an expedited process whereby once stakeholders file a petition, the government that receives the complaint has 30 days to notify petitioners whether the government will activate the mechanism based on their complaint. If the government has a good-faith belief that workers' rights are being denied at the targeted facility, it will move forward with the labor rights violation complaint and ask Mexico to conduct a review. Upon receipt of the request for review, Mexico has 45 days to assess the situation and accept (or deny) that a violation of rights is taking place.

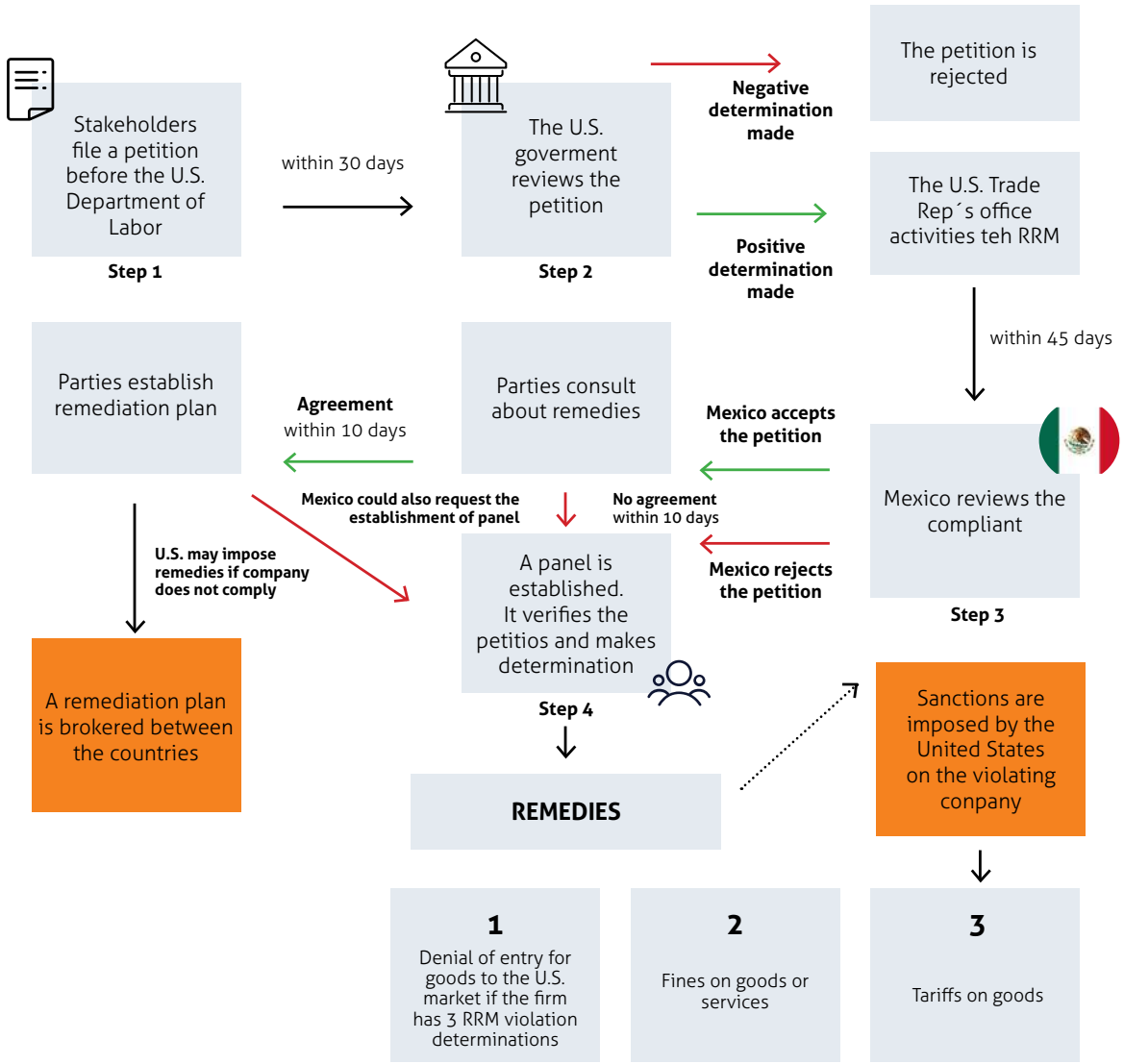
In principle, the Mexican government and the complaining governments will establish a plan to remediate the violations if Mexico accepts that a Denial of Rights is taking place. If Mexico denies the allegations or the governments cannot mutually agree on a remediation plan, the United States or Canada have the right to invoke a panel. Under the RRM, a panel composed of three labor experts selected by the respective governments determines whether a Denial of Rights has occurred and, if so, authorizes the imposition of sanctions by the United States or Canada. These sanctions include loss of preferential tariff treatment for goods manufactured at the specific facility or penalties on the goods or services provided by the facility.

[10] Desiree LeClercq, "The U.S. 'Worker-Centered Trade Policy' Is Helping Some Workers in Mexico but Not in America," International Economic Law and Policy Blog, September 3, 2023, https://ielp.worldtradelaw.net/2023/09/the-us-worker-centered-trade-policy-is-helping-some-workers-in-mexico-but-not-in-america.html.

[11] Desiree LeClercq, "The U.S. 'Worker-Centered Trade Policy' Is Helping Some Workers in Mexico but Not in America," International Economic Law and Policy Blog, September 3, 2023, https://ielp.worldtradelaw.net/2023/09/the-us-worker-centered-trade-policy-is-helping-some-workers-in-mexico-but-not-in-america.html.

When a company faces repeated complaints under the RRM, the agreement envisions an escalated system of penalties. Thus, if a facility or a facility owned or controlled by the same company or person receives a second Denial of Rights Determination, the U.S. or Canadian government may impose escalating penalties. And if the same facility or a facility owned or controlled by the same person receives a third Denial of Rights Determination, the company could face a ban on its exports.

The graphic below shows the stages and the ideal outcomes of the RRM.



The RRM in Practice:

How Has Facility-Specific Labor Enforcement Worked So Far?

This report analyzes the practical outcomes of the RRM over its first five years in existence. It focuses on the cases in which the U.S. government requested that the Mexican government conduct a review because there is very limited public information about petitions that were not accepted by the U.S. government. However, before turning to the outcomes of the cases initiated by the United States, Box 1 below underscores the critical need to scrutinize unsuccessful RRM petitions. Neglecting them risks weakening the credibility and effectiveness of the mechanism. However, information about why these petitions did not proceed and even how many petitions have been filed is not publicly available at present.

BOX 1: Unsuccessful RRM Petitions: What FOIA Told Us (and What It Didn't)

The lack of public information on petitions that did not advance to a request for review is a primary reason this analysis focuses on cases that reached at least the respondent's review stage. There is virtually no public information about filed petitions that did not progress to a request for review.

As previously noted, it was only through a FOIA request that we learned 56 petitions were filed with the U.S. government in the first five years of the RRM, since neither the United States nor Mexico publish information on petitions that do not result in a request for review by the complainant Party. (See Appendix for a list of the petitions disclosed.) Of those 56 petitions, 36 led to a request for review from the U.S. government to its Mexican counterparts. Additionally, the United States self-initiated two cases (General Motors Silao and Draxton) and one petition was withdrawn, according to Department of Labor (DOL). This means that 19 petitions were rejected or otherwise failed to trigger the activation of the mechanism. There is little publicly available information explaining why these petitions did not advance. According to DOL's FOIA response, there is a distinction between petitions that are "accepted" and those that proceed to the next step, a request for review. In response to a clarifying question related to the previously mentioned FOIA request, the Bureau of International Labor Affairs (ILAB) stated:

"When DOL receives a Rapid Response Mechanisms petition, ILAB must first determine whether it meets the following procedural requirements:

- *Whether the claim includes freedom of association violations or the right to bargain collectively, heretofore referred to as Denial of Rights (DOR)*
- *Whether the petitioner provided the name and address of the facility*
- *Whether the petitioner provided contact information*

If the petition does not meet the procedural requirements, it is rejected. If it does meet those requirements, it is accepted, and the 30-day investigation timeframe begins. At the conclusion of the 30-day investigation period, not all accepted RRM petitions result in referrals to the Government of Mexico for review."

The legal basis for the procedural requirements test mentioned by DOL is not apparent from either the USMCA text or the Final USMCA Procedural Guidelines issued by USTR in 2023.[12] Increasing awareness among petitioners and prospective petitioners about the methodology used by the agencies administering the mechanism would improve stakeholders' understanding of the process and likelihood of success.

Regarding the information disclosed by DOL, of the 19 petitions that did not reach a request for review, eight were rejected for failing to meet the procedural requirements outlined by ILAB. The remaining 11 petitions were accepted and investigated but ultimately did not lead to a request for review.

There is virtually no information explaining the U.S. government's decision not to activate the mechanism in these cases, nearly one quarter of accepted petitions. It is worth recalling that policymakers designed and supported the mechanism under the assumption that there would be a low threshold for workers to initiate an investigation and achieve remediation. For instance, U.S. Senator Sherrod Brown (one of the RRM's architects), while explaining on the Senate floor why he thought the mechanism would be effective, said: *"(...) one of the things we knew would speed it up (...) and would mean that enforcement would work was that the workers would have an ability to kick off the investigation, to literally call a toll-free number. They can register that they have seen (...) workers attacked, violence aimed against workers; that they have seen wages denied for all kinds of illegal reasons. So workers can speak out and band together and go to a panel and get quick action."*[13]

Thus, although the success rate has been high—35 of 46 accepted petitions led to a request for review—understanding why nearly one quarter did not advance could help petitioners craft more effective strategies and better align with policymakers' intentions. Additionally, it would promote accountability in instances where the government decision not to proceed might be questionable. Addressing this lack of transparency should be a key objective of the 2026 review.

[12] Federal Register, National Archives, "Notice of Interagency Labor Committee for Monitoring and Enforcement Final Procedural Guidelines for Petitions Pursuant to the USMCA," Office of the United States Trade Representative, June 22, 2023, https://www.federalregister.gov/documents/2023/06/22/2023-12865/notice-of-interagency-labor-committee-for-monitoring-and-enforcement-final-procedural-guidelines-for.
[13] Senator Brown, speaking on H.R. 5430, on January 15, 2020, 116th Congress, 2nd sess., Congressional Record Vol. 166, No. 9, S228, https://www.govinfo.gov/content/pkg/CREC-2020-01-15/pdf/CREC-2020-01-15-senate.pdf.

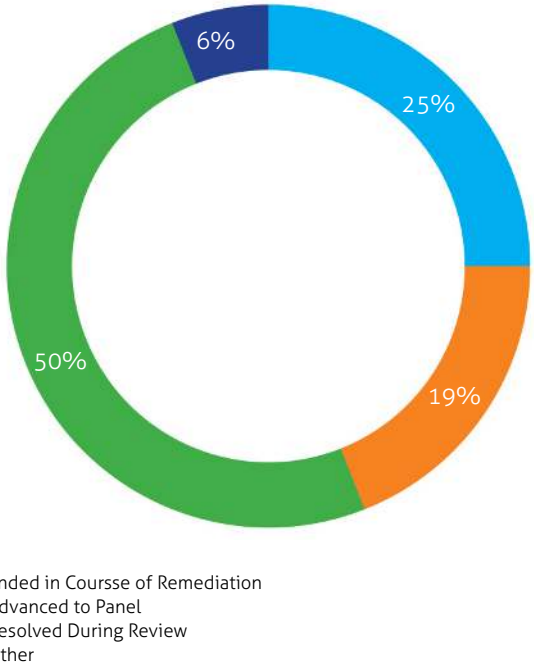
Critically analyzing both the procedural and substantive outcomes of the cases launched under this novel labor enforcement mechanism is essential to prioritizing necessary improvements during the 2026 USMCA review. Procedural outcomes take into consideration how each of the cases was concluded or terminated, and we discuss the potential effects of the trends observed. Substantive outcomes refer to the types of remediation that have resulted from RRM cases. To evaluate substantive outcomes, we identified and coded the specific remedial actions that resulted from the initiation of an RRM case. There are certain remedial actions that are much more prevalent than others, which arguably impacts the RRM's ability to protect workers' rights to freedom of association and collective bargaining. Finally, we assess the RRM's impact on representation, bargaining, and wages to better understand the mechanism's real effects on achieving independent union representation, improving collective bargaining, and raising workers' wages at the offending facilities.

Procedural Outcomes

As noted above, the initial phase of an RRM case should ideally end either with a formal Course of Remediation or a request to establish a panel. Once a panel has been established, it must determine whether a Denial of Rights has taken place. If the panel makes a positive determination, the complaining government is authorized to apply sanctions on the offending facility. As of August 2025, there have only been two panel decisions: *San Martín Mine* and the recently published *Atento Servicios*. In the *San Martín Mine* case, the panel decided that it did not have jurisdiction over the matter at hand. By contrast, in the *Atento Servicios* case, the panel issued its report in August 2025, confirming that the company had indeed denied workers' rights at a covered facility. This groundbreaking decision was released only weeks before the publication of this report. The report does not provide a thorough analysis of its implications, particularly given that the decision's potential ramifications for remediation of the Denial of Rights found by the panel have yet to be seen.

Accordingly, our analysis focuses on pre-panel outcomes, classifying the cases in four categories: (a) cases which ended in a Course of Remediation; (b) cases which led to the activation of a panel; (c) cases "resolved during review," which means that the governments determined that the alleged violations were remedied during the investigation; or (d) other.

Figure 2. Pre-Panel Outcomes of known RRM Cases

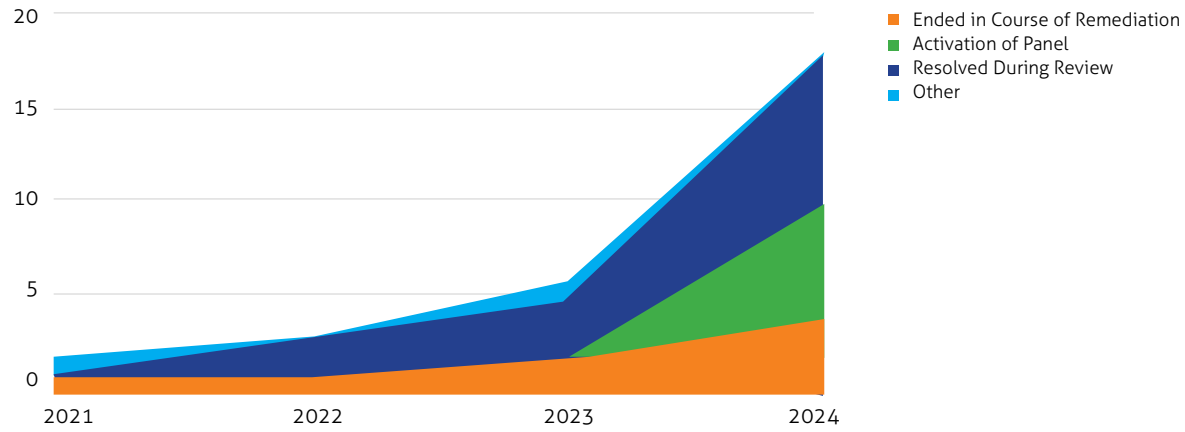


Of the 32 cases that concluded the pre-panel phase by June 30, 2025, half of them, 16, were "resolved during the review" according to the U.S. and Mexican governments. Eight cases ended with a formal Course of Remediation, six led to the establishment of a panel, and two had another type of outcome. For instance, in the *Tridonex* case, USTR reached an agreement directly with the facility given that the government of Mexico refused to accept the Denial of Rights claim.

As noted previously, ideally, the RRM pre-panel phase should lead to one of two outcomes: either the governments agree on a Course of Remediation or the complaining government requests the establishment of a panel. In practice, however, an increasing number of cases are closed before either outcome occurs. Instead, the governments announce that the case was "resolved during review." As the graph above shows, half of all RRM cases that the United States has launched fall under this category. In these cases, the companies involved carried out some remediation actions that, in the governments' eyes, were sufficient to address the Denial of Rights that triggered the activation of the mechanism and, therefore, a formal Course of Remediation was not required.

This scenario poses significant challenges. It is not clearly outlined in the RRM procedural rules. Yet it has become evident that, over time, the Mexican government began to see the value in resolving cases before they could result in a formal Course of Remediation. No cases were resolved during review in the RRM's first year in 2021. In 2022, two cases were resolved during review, while only one resulted in a Course of Remediation. In 2023, there were two Courses of Remediation and three cases resolved during review. In 2024—the year with most RRM activity so far—nine cases were resolved during review, while only four Courses of Remediation were agreed between the governments of the United States and Mexico. The three cases that concluded in the first half of 2025 were resolved during review, with no recourse to a panel or a Course of Remediation since the start of the new Trump administration.

Figure 3. Outcomes of U.S. RRM Complaints (2021-2024)



One likely explanation for this trend has its basis in the "three-strike system" adopted by Annex 31-A of the USMCA. Recall that, once the first Denial of Rights has been determined, the complainant Party will select a remedy, which may include "suspension of preferential tariff treatment for goods manufactured at the specific Covered Facility" or "imposition of penalties" on goods or services provided by the Covered Facility.[14] After a second Denial of Rights determination, these remedies can be extended to other Covered Facilities owned or controlled by the same entity.[15] A third finding of Denial of Rights allows the complainant Party to completely prohibit entry of goods from the entity that owns the facility, including other Covered Facilities that have not been the subject of dispute.[16]

One concern with a high number of cases ending with a "resolved during review" decision is that it is unclear whether this kind of outcome would be interpreted as a Denial of Rights Determination for the purposes of the RRM's escalating sanction system.

> By resolving cases before a Course of Remediation can be reached, Mexico, along with the noncompliant company, might be trying to avoid an admission of a Denial of Rights and, thus, the imposition of a "first strike."

Another design feature that may be contributing to the prevalence of "resolved during review" outcomes is the way the text of the agreement and the United States' implementing legislation for the pact interact with respect to timelines. The USMCA Implementation Act requires that the Interagency Labor Committee decide whether to request the establishment of a panel within 60 days of invoking the RRM.[17] Given the timeline for the rest of the process set forth in the pact, this gives the U.S. government only 15 days after Mexico's 45-day internal review period ends to determine whether to advance the case. It is unlikely that the Interagency Labor Committee has sufficient time during this window to fully assess the effectiveness of a company's remedial actions or its commitment to respect labor rights after being targeted under the RRM. As a result, the tight deadline may pressure the Committee to forgo initiating a panel and instead accept that the complaint has been "resolved during review" even before it can accurately determine whether the Denial of Rights has truly been remedied.

[14] "United States-Mexico-Canada Agreement," conclusion date: November 30, 2018, Art. 31-A.10.2, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/31-Dispute-Settlement.pdf.
[15] USMCA, Art. 31-A.10.4.
[16] Jamieson Greer, Christopher Hyner, Mercedes Morno, J. Michael Taylor, and Patrick Togni, "Companies Face Risk From The USMCA's New Rapid Response Mechanism To Enforce Labor Rights ," *JD Supra*, July 16, 2020, https://www.jdsupra.com/legalnews/companies-face-risk-from-the-usmca-s-40266?utm.
[17] U.S. House, United States-Mexico-Canada Agreement Implementation Act USMCA Implementation Act, HR 7520, 116th Congress, 2nd sess., introduced in House December 13, 2019, Section 716(b)(4), https://www.congress.gov/bill/116th-congress/house-bill/5430/text.

This dynamic may help explain cases in which a facility has been targeted by subsequent petitions. According to the FOIA information we obtained, three facilities faced at least a second petition after the initial case was "resolved during review." In one instance, *Manufacturas VU* chose to close the facility rather than comply with the Course of Remediation established through the second complaint.[18] In another, *Tecnología Modificada (Caterpillar)*, workers have been on strike for two years while being blacklisted, and a second RRM petition was not effective in resolving the labor dispute.[19] It is worth considering whether these outcomes could have been avoided if the initial cases had not been deemed "resolved during review" and, instead, the companies had been required to implement a formal Course of Remediation under the threat of sanctions for non-compliance.

Closing cases prematurely is deeply problematic given the power imbalance between workers and employers. During a conflict, workers are often on strike, dismissed, blacklisted, and in some cases even threatened or assaulted. For employers, active RRM cases may be inconvenient, but they typically have the resources to withstand prolonged disputes. As a result, when corporations can extend conflicts and avoid having a "strike" on their record, even while facing multiple RRM investigations, workers' incentives to defend their rights and interests are severely weakened.

All this suggests that, while cases being "resolved during review" might initially sound like a positive development, this outcome could in fact shield companies from facing real sanctions under the RRM. This trend is particularly concerning if the commitments and actions resulting from an RRM case are not substantial enough to meaningfully address the underlying labor rights violations. To evaluate this possibility, the next subsection examines the types of remediation achieved through the RRM.

Types of Remediation

While the USMCA text explicitly states that the primary goal of the mechanism is to ensure remediation of Denials of Rights,[20] the agreement does not define what constitutes effective remediation. Moreover, given the diversity of situations that have triggered Denial of Rights complaints, it is hard to determine which kind of actions should be considered enough to bring the facility back into compliance. This report identifies the most common remedial actions achieved through RRM cases, as announced by the governments when signing a Course of Remediation or announcing that a case has been "Resolved During Review."

Table 1 lays out the most common remediation actions announced by the governments through Courses of Remediation or "Resolved During Review" decisions.

[18] "Statement by Undersecretary of Labor for International Affairs Thea Lee on Closure of Auto Parts Facility Accused of Labor Rights Violations at Piedras Negras Plant in Mexico," U.S. Department of Labor, Bureau of International Labor Affairs, October 10, 2023, https://www.dol.gov/newsroom/releases/ilab/ilab20231010.

[19] Noam Scheiber, "Caterpillar Factory in Mexico Draws Complaint of Labor Abuses," *New York Times*, July 15, 2024, https://www.nytimes.com/2024/07/15/business/economy/uaw-usmca-mexico-trade-caterpillar.html.

[20] USMCA, Art. 31-A.11.2.

Table 1. Top 10 Most Common Remediation Actions Achieved through the RRM

Common Remedial Actions	Total Number of Cases
Neutrality Statement and/or Zero-Tolerance Policy	26
Mexico-Provided FOA Training	24
Facility-Provided FOA Training	19
Worker Reinstatement and/or Backpay	19
Anonymous Hotline to Report Violations	14
Severance Payments	7
Union Access to Facility	7
Proper Management of Union Dues	6
CBA Distribution	5
Recognizing and Engaging in Bargaining with Petitioner Union	5

As evidenced by Table 1, the vast majority of RRM cases so far have led to the adoption of neutrality statements (public statements that commit the offending company to respect workers' rights to freedom of association and collective bargaining) and the issuance of a zero-tolerance policy, which is supposed to guarantee management's adherence to the neutrality statement. Additionally, a remedy found in most cases is Mexico's commitment to conduct in-person freedom of association (FOA) trainings for all company personnel. While useful, a report published by Cornell University shows that worker training programs triggered by RRM complaints have not been sufficient to promote workers' awareness about the labor law reforms, the process to approve their collective bargaining agreements, or union election procedures.[21] Additionally, the aforementioned cases in which one facility has been targeted by multiple RRM petitions raise questions about the effectiveness of neutrality statements and zero-tolerance policies as remedies against union-busting conduct. Indeed, in the *Atento Servicios* case, the panel found that, despite adopting a neutrality statement, the company continued to favor the employer-controlled union—demonstrating that the mere adoption of such a statement did not amount to genuine remediation.[22]

Thus, a more significant development is that, in 19 cases, offending facilities have been required to reinstate workers who were dismissed in retaliation for their union activism and provide them with backpay.

> Reinstating and making whole workers who were unjustifiably fired is a crucial way to uphold labor rights, and the use of this remedy in nearly two-thirds of the concluded RRM cases stands out as one of the system's most significant achievements.

[21] Desirée LeClercq, Alex Covarrubias-V, and Cirila Quintero Ramírez, "Enforcement of the United States-Mexico-Canada Agreement ('USMCA') Rapid Response Mechanism: Views from Mexican Auto Sector Workers," Cornell University, ILR School, January 2024, https://ecommons.cornell.edu/items/989323d0-4f38-4947-ab7c-706c0a72ea1c.

[22] Panel's Final Determination, *Rapid Response Labor Panel on the Atento Servicios Case* (MEX-USA-2024-31A-01), July 4, 2025, para. 426.

However, other remedial actions that support workers in organizing and negotiating better wages have been less common. In only seven cases were companies required to facilitate the petitioner union's access to the facility's premises. Notably, one of the grounds on which the panel in *Atento Servicios* deemed remediation insufficient was that the minority union—the petitioner in the case—was denied access to the facility even after both the U.S. and Mexican governments had found a serious Denial of Rights.[23] Similarly, in just five cases *(Panasonic, Manufacturas VU II, Minera Tizapa, Odisa Concrete, and Modern Metal Alloys)*, a commitment by the company to recognize the petitioner union as the workers' bargaining representative was included as part of the remediation.

The low number of cases in which a commitment to recognize and bargain with the petitioner union was included as part of the remediation may be attributed to a perceived gap in Mexican labor law. Unlike labor laws in the United States and Canada, Mexico's Federal Labor Law does not explicitly impose a legal duty on employers to bargain in good faith.[24] Yet, since the enactment of the 2019 reform, the newly established Mexican labor courts have begun to recognize the principle of bargaining in good faith, which is derived from the obligation to promote collective bargaining set out in Article 4 of ILO Convention No. 98.[25] However, the application of the principle of bargaining in good faith so far appears to have been limited to cases where an employer violated obligations under an existing CBA,[26] rather than to situations showing a lack of good-faith bargaining to secure an initial contract. As a result, Mexican labor law enforcement does not typically address bargaining practices or an employer's refusal to negotiate. Instead, enforcement focuses on guaranteeing the right to strike. In these cases, the role of the labor authorities is limited to verifying that the strike meets legal requirements and, if so, enforcing the right to strike by providing the workers with the necessary guarantees and support to halt company operations.[27]

[23] Panel's Final Determination, *Rapid Response Labor Panel on the Atento Servicios Case*, para. 428.

[24] In the United States, while the National Labor Relations Act requires parties to bargain collectively in good faith, legal scholars have noted gaps in both its definition and application that should be addressed. See Colleen McMullen, "Good Faith in Collective Bargaining: A Term Without Concrete Meaning," Penn State Law Review, April 14, 2023, https://www.pennstatelawreview.org/the-forum/good-faith-in-collective-bargaining-a-term-without-concrete-meaning/.

[25] International Labour Office, "Freedom of Association and Collective Bargaining: General Survey," Report III (Part 4B), Chapter III, International Labour Conference, 81st Session, 1994, accessed August 22, 2025, https://webapps.ilo.org/static/english/dialogue/ifpdial/llg/noframes/ch3.htm#ref_27.

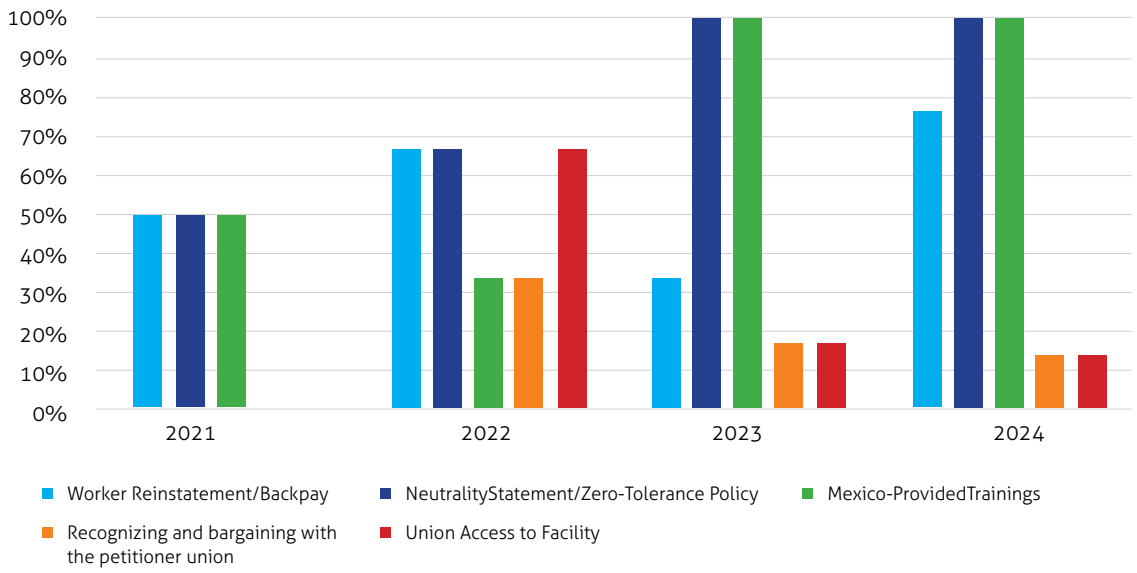
[26] Sindicato Independiente de Trabajadores de "La Jornada" v. DEMOS, Desarrollo de Medios, S.A. de C.V., Procedimiento especial colectivo 639/2024 (Tribunal Laboral Federal de Asuntos Colectivos, Mexico City, 3 July 2024); Unión del Personal Académico del CINVESTAV v. Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, Procedimiento especial colectivo 863/2024 (Tribunal Laboral Federal de Asuntos Colectivos, Mexico City, November 5, 2024).

[27] "U.S. and Canadian labor laws establish a legal 'duty to bargain in good faith' on the part of employers. Unlike Canadian and U.S. labor law, Mexican labor law does not create a legal duty to bargain. Mexican labor law enforcement thus does not deal with negotiating practices or refusals to bargain per se. Rather, legal enforcement deals with the results of an employer's refusal to sign the contract sought by the union, if the refusal results in a strike. The legal enforcement role of the CAB in these situations is to verify that the strike meets legal requirements and, if so, to enforce the right to strike by granting the workers the necessary guarantees and assistance to halt company operations." Kevin Banks, Lance A. Compa, Leoncio Lara, and Sandra Polaski, "Labor Relations Law in North America," Commission for Labor Cooperation, 2000, p.123, https://ecommons.cornell.edu/items/92cbdd9d-448c-4e24-968d-40e353d0b97b.

Still, it is worth noting that in the first year of consistent RRM activity (2022), the U.S. and Mexican governments were able to secure commitments from companies in 67% of cases to grant the petitioner union access to the facility's premises, and in 33% of cases to recognize and bargain with the petitioner union. These percentages fall to 17% and 15% in 2023 and 2024, respectively, for each of these types of remedies. Only one of the three concluded cases in the first half of 2025 included remediation measures in which the company committed to grant the petitioner union access to the facility's premises and to recognize and engage in collective bargaining.

Conversely, all cases that produced remedial measures since 2023 have required the Covered Facility to implement a neutrality statement and/or zero-tolerance policy and have assigned the Mexican government to provide training to personnel. This pattern suggests that such remedial actions have become standardized even if they may be insufficient to effectively address violations or deter future breaches, as the *Atento Servicios* case showed.

Figure 4. Share of Remedial Actions in Concluded Cases by Year



Impact on Representation, Bargaining, and Wages

While immediate remedial actions are important, the ultimate measure of the RRM's success is whether workers achieved independent representation and the ability to collectively bargain for higher wages and improved working conditions after filing an RRM case. Thus, based on public information, this report analyzes whether the filing of an RRM case led to: (a) workers securing the right to be represented by a new union; and (b) the union successfully negotiating or revising a CBA.

Table 2. Union Representation and Collective Bargaining Outcomes of Concluded RRM Cases by Workplace

Workers gained new union representation and/or a new/ revised CBA	Workers only gained new union representation	RRM activity did not result in new union representation or a new/ revised CBA
1. General Motors (2021)	1. Manufacturas VU (2022)	1. Draxton (2023)
2. Tridonex (2021)	2. Unique Fabricating (2023)	2. Grupo México – San Martín mine (2023)
3. Panasonic (2022)		3. Grupo Yazaki (2023)
4. Teksid Hierro (2022)		4. Asiaway Automotive Components (2023)
5. Goodyear (2023)		5. Tecnología Modificada – Caterpillar (2023)
6. INISA (2023)		6. Fujikura* (2023)
7. Aerotransportes MAS de Carga (2023)		7. Atento Servicios (2024)
8. Teklas (2023)		8. RV Fresh Foods* (2024)
9. Autoliv (2023)		9. Servicios Industriales González (2024)
10. Minera Tizapa (2024)		10. Volkswagen* (2024)
11. Odisa (2024)		11. Impro (2024)
12. Modern Metal Alloys (2025)		12. Vidrio Decorativo Occidental (2024)
		13. Aludyne Automotive (2025)
		14. Superior Industries (2025)

Table 2 classifies concluded RRM cases based on this analysis (the year in parenthesis indicates the year in which the case was initiated by the U.S. government). It shows that at least in 12 cases, RRM activation with regards to a workplace led to new union representation and/or the negotiation of a new or revised CBA. However, in 14 cases, there is no evidence of RRM activity leading to new union representation or the negotiation of better wages and working conditions.

Importantly, not all RRM cases have been filed with these ultimate objectives. For instance, the case against the *Volkswagen* facility located in Puebla was not related to workers' struggle to gain better union representation or achieve a new or improved CBA. The Volkswagen Puebla plant has been represented by an independent union since the early 1970s. The RRM petition alleged Volkswagen dismissed former members of the union's Executive Board in retaliation for union activity they conducted while serving as union representatives.[28] The cases marked with an asterisk in the table are those in which securing new union representation or a new or improved collective bargaining agreement was likely not the petitioners' ultimate goal when filing the complaint.

The fact that half of all concluded RRM cases have not resulted in new union representation and/or a new or revised contract raises questions about the mechanism's effectiveness in fulfilling its ultimate objectives. Box 2 delves into one of the cases where, despite the initiation of the RRM, workers' efforts to gain representation by an independent union were obstructed.

BOX 2: Draxton: How 62% of Workers Voting for an Independent Union Did Not Result in New Union Representation

Draxton is a global company with operations in six countries on three continents, including North America.[29] This company has three factories in Mexico, with one plant located in Irapuato, Guanajuato.[30] Workers at this plant make iron and aluminum parts for carmakers such as Chrysler, Ford, and Audi. The Irapuato factory began operations in 2004 and employs nearly 500 workers.[31]

USTR self-initiated an RRM case against Draxton's Irapuato facility on May 31, 2023, after receiving information concerning several serious denials of labor rights, including the termination of a union official and company interference with workers' activities in order to control the union.[32] This case was the fourth time the U.S. government initiated the RRM and only the second-ever self-initiated case. USTR specifically expressed concern that

[28] "United States and Mexico Announce Course of Remediation at Volkswagen de México Facility," Office of the United States Trade Representative, July 30, 2024, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2024/july/united-states-and-mexico-announce-course-remediation-volkswagen-de-mexico-facility.
[29] "Rapid Response Labor Mechanism: Draxton Case," Vázquez Tercero & Zepeda, last modified June 2, 2023, https://vtz.mx/the-trading-room/draxton-rapid-response-labor-mechanism/.
[30] "Labor Complaint Closed at Draxton Plant in Irapuato, Guanajuato," *Mexico Daily Post*, August 2, 2023, https://mexicodailypost.com/2023/08/02/labor-complaint-closed-at-draxton-plant-in-irapuato/.
[31] "Rapid Response Labor Mechanism: Draxton Case," Vázquez Tercero & Zepeda.
[32] "United States Announces Successful Resolution of Rapid Response Labor Mechanism Matter at Draxton Facility," Office of the United States Trade Representative, April 9, 2024, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2024/april/united-states-announces-successful-resolution-rapid-response-labor-mechanism-matter-draxton-facility; Article 132.XXX of the Federal Labor Law requires each employer to "Deliver to its workers, free of charge, a printed copy of the initial collective bargaining agreement or of its revision within fifteen days after such agreement is deposited with the Federal Center for Labor Conciliation and Registration; this obligation may be evidenced by the worker's signature of receipt."

Draxton was privileging *Sindicato Nacional de Trabajadores de la Industria Metalmecánica y del Acero ("Lic. Benito Pablo Juárez García") and interfering with the activities of the independent union, Sindicato Independiente Nacional de Trabajadores y Trabajadoras de la Industria Automotriz* (SINTTIA).[33] An investigation by USTR found that workers experienced harassment, surveillance, and intimidation when they tried to join SINTTIA.[34] One source reported that a SINTTIA official faced threats and violence at his home.[35] The U.S. government also found that workers voted on a CBA in 2022 without receiving it first and still have not received it.[36]

The Mexican government agreed to conduct its own review and concurred with USTR's findings. On July 14, 2023, it announced that there were ongoing denials of the rights to free association and collective bargaining at the facility. The United States and Mexico announced a Course of Remediation on July 31, 2023, with a deadline of October 30, 2023, to complete all the remedial actions.[37] Under the Course of Remediation, Mexico was supposed to undertake several actions to ensure the Draxton facility was not involved in future violations, including overseeing the reinstatement of the union official who was unlawfully dismissed. Actions to be taken by Mexico also included conducting in-person workers' rights training for all company personnel; offering an anonymous hotline to report any intimidation, coercion, or threats with respect to union activities; monitoring and visiting the facility prior to any union vote to ensure workers have awareness of the CBA; and initiating sanctions proceedings if Mexican government officials had information showing violations of Mexican law.

After the announcement of the Course of Remediation, SINTTIA filed a lawsuit to contest the control of the CBA. This action led to a worker vote on November 30 and December 1, 2023, to decide which union they wanted to represent them. The vote was monitored by the International Labor Organization (ILO), independent observers, and the Mexican Secretariat of Labor and Social Welfare. According to SINTTIA, the company-controlled union tried to rig the election, creating a smear campaign against it and "buying votes, spreading lies, and altering propaganda of the independent union."[38] Nevertheless, once the ballots were tallied, SINTTIA received 61.7% of the vote and was confirmed as the union designated to represent the workers in collective bargaining.[39]

Despite its electoral victory, SINTTIA was not able to represent Draxton workers and negotiate a new CBA because the company-controlled union filed an injunction (*"amparo"*) to contest the outcome of the vote. The claim rested on an allegation that SINTTIA's lawsuit lacked a secondary signature. The Federal Labor Court specialized in collective bargaining matters assessed this claim, found

[33] "Rapid Response Labor Mechanism: Draxton Case," Vázquez Tercero & Zepeda.
[34] "United States Announces Successful Resolution of Rapid Response Labor Mechanism Matter at Draxton Facility," USTR.
[35] "Rapid Response Labor Mechanism: Draxton Case," Vázquez Tercero & Zepeda.
[36] "United States Announces Successful Resolution of Rapid Response Labor Mechanism Matter at Draxton Facility," USTR.
[37] Course of Remediation: Draxton Facility, Office of the United States Trade Representative, July 28, 2023, https://ustr.gov/sites/default/files/2023%2007%2028%20COR%20Draxton.pdf.
[38] Jared Laureles, "Trabajadores de Draxton Elegirán en Votación a Representación Sindical," La Jornada, November 23, 2023, https://www.jornada.com.mx/noticia/2023/11/23/sociedad/trabajadores-de-draxton-elegiran-en-votacion-por-representacion-sindical-7680.
[39] Verónica Gascón, "Se Aferra Sindicato Propatronal a Draxton," *Reforma*, August 6, 2024, https://www.reforma.com/se-aferra-sindicato-propatronal-a-draxton/ar2852648.

that the alleged deficiency was immaterial, and granted SINTTIA the right to represent Draxton workers.[40] While the challenge was ongoing, the Federal Labor Court's decision was stayed, meaning that the company-controlled union retained control over the CBA covering this plant. Despite the fact that workers were being denied the right to representation by the union they had elected, the United States announced the resolution of the USMCA RRM case in April 2024.[41] Eventually, the court charged with deciding the *amparo* ruled in favor of the *"Lic. Benito Pablo Juárez García"* union, overturning the specialized Federal Labor Court's decision. When the *amparo* reached Mexico's Supreme Court in August 2024, the Court declined to hear the case, effectively siding with the company-controlled union and invalidating the vote. To this date, the company-controlled *"Lic. Benito Pablo Juárez García"* union controls the CBA covering this facility.

While *Draxton* is undoubtedly a complex case with no easy answers, it is a useful case study to explore how the activation of the RRM could have been more effective in addressing the violations and promoting the right to freedom of association at this facility. To begin with, it is important to note that this case concluded with a formal Course of Remediation, thereby avoiding the pitfall of being "resolved during review"—a positive development. However, the Course of Remediation negotiated by the U.S. and Mexican governments imposed a very short deadline: Remediation actions were expected to be completed within three months. As a result, by the time the judicial process triggered by SINTTIA's CBA control challenge concluded, the remediation timeline had already expired.

Moreover, while the Course of Remediation required Mexico to ensure compliance with the law if a union-related vote was held at this facility, it did not account for potential legal challenges to the outcome of such a vote. Under the RRM, a Denial of Rights may be permitted—or even perpetuated—by administrative or judicial authorities. For this reason, Courses of Remediation could include guarantees that the Respondent Party's authorities will not obstruct workers' rights to freedom of association and collective bargaining. If an independent panel determines that this obligation has not been met, sanctions should be imposed on the facility concerned. Admittedly, when the Draxton Course of Remediation was negotiated, it was difficult to foresee the events that led domestic courts to dismiss SINTTIA's electoral victory. However, after five years of RRM experience, the way in which certain courts and administrative bodies appear to obstruct workers' rights to organize and bargain collectively indicates that greater attention must be paid to government conduct as a potential enabler—or even primary source—of denials of rights.

[40] Jared Laureles, "Pretende Tribunal Anular Fallo del T-MEC Sobre CCT en Empresa de Autopartes," *La Jornada*, August 9, 2024, https://www.jornada.com.mx/2024/08/09/politica/012n1pol.
[41] "United States Announces Successful Resolution of Rapid Response Labor Mechanism Matter at Draxton Facility," USTR.

During the first two years of the RRM (2021 and 2022), all five cases led to new union elections, and four cases led to successful negotiation of a CBA and increased wages for workers. This impressive success rate dwindles in 2023 and 2024, with fewer cases resulting in new union representation and/or better contracts. Two factors could be contributing to this trend. First, it is likely that corporations—and the law firms representing them in these cases—have developed strategies to convince the authorities that certain actions constitute sufficient remediation without actually allowing workers to organize in independent unions. Relatedly, in 2023 and 2024, the share of cases that were decided to be "resolved during review" increased markedly. Since this means that cases are closed more quickly, corporations are emboldened to obstruct workers' organizing and bargaining efforts when the authorities are no longer actively investigating them. The 2026 USMCA review must include changes to reverse this pattern.

Policy Recommendations for the 2026 USMCA Review

The RRM has arguably been the most significant development in the trade and labor field in decades. Moreover, the U.S. government's active use of this novel tool has demonstrated that labor-related trade-enforcement mechanisms can deliver tangible benefits for workers and help level the playing field. To ensure this continues—and to enhance the mechanism's effectiveness—several changes should be considered in the upcoming 2026 review. Based on the findings in this report, we recommend a set of targeted adjustments and broader systemic improvements:

Targeted Adjustments

1. Shorten the respondent Party's period for internal review: Currently, the respondent Party—Mexico in all cases to date—has 45 days to conduct an internal review of Denial of Rights allegations. However, U.S. government practice has shown that it is feasible to complete such investigations within 30 days. Given that the Mexican government has greater access to relevant facilities and investigative tools, the need for a longer review period is questionable. More importantly, the growing number of cases categorized as "resolved during review" suggests that the internal review period is often used by companies to take quick, surface-level actions to address the most visible violations. In many instances, this has not meaningfully remedied the underlying barriers to workers' rights to organize and bargain collectively.

   Shortening the internal review period to 30 days—aligning it with the complainant Party's timeline—could encourage the respondent Party to focus on conducting a substantive evaluation of alleged violations rather than spending time trying to rapidly close cases without systemic fixes.

2. Extend or modify the Interagency Labor Committee's deadline to determine whether to invoke a panel: While the USMCA itself does not impose a deadline for the Complainant Party to request the establishment of a panel, the U.S. USMCA Implementation Act added a requirement that the Interagency Labor Committee must decide whether to request a panel within 60 days of invoking the RRM. As

a result, the U.S. government has only 15 days after Mexico's 45-day internal review period ends to determine whether to advance the case.

The intent behind this deadline is commendable—it aims to prevent indefinite delays in pursuing cases where labor rights violations persist. However, the time constraint may inadvertently contribute to the premature closure of cases based on remedial actions that fall short of ensuring fair organizing and bargaining conditions over the medium to long term.

To address this, Congress should consider modifying the deadline to give the Interagency Labor Committee sufficient time to assess the implementation and impact of remediation commitments before forgoing the option of requesting a panel. This could be achieved by either extending the deadline by an additional 15 to 45 days or by allowing the Committee to extend its own deadline in cases where further time is necessary to evaluate the effectiveness of corrective measures.

3. Require Parties to meaningfully consult with stakeholders—particularly the petitioners—when discussing remediation actions, and mandate that investigating authorities disclose the outcomes of their findings to stakeholders: The RRM obliges Parties to engage in consultations to agree on a Course of Remediation but is silent on the role stakeholders should play during this stage. Requiring authorities to conduct meaningful consultations with stakeholders—including the noncompliant company but, above all, the petitioners—would increase the likelihood that remediation measures fully address the violations experienced by workers. This is especially important because violations often continue after an RRM case has begun, and petitioners should be able to supplement the information provided at the time of filing.

In addition, the Parties should be required to communicate in writing the findings of their investigations to relevant stakeholders, while withholding any information that could endanger workers. Doing so would improve stakeholders' understanding of the mechanism and strengthen the overall functioning of the RRM.

4. Clarify that a "Resolved During Review" outcome counts as a Denial of Rights Determination: The RRM enforcement mechanism is built on a system of escalating penalties. Increasing the potential costs of labor rights violations is essential to deterring such behavior. Hence, it is crucial to ensure that corporations involved in violations have their records effectively impacted and clearly face a heightened risk of subsequent RRM cases. In this context, the growing trend of cases being labelled as "resolved during review"—and the possibility that the respondent government and involved companies may be pushing for this outcome to avoid receiving a "first strike"—warrants immediate attention.

A straightforward way to address this concern would be to clarify in the USMCA text that a case resolved during the review phase still constitutes a Denial of Rights Determination for the purposes of the penalty system outlined in Article 31-A.10 of the agreement.

5. Clarify that administrative and judicial authorities' actions can constitute a Denial of Rights under the RRM: The USMCA text does not impose an "attribution" requirement.[42] This means that for a facility to face sanctions under the RRM, it is not necessary to attribute the denial of workers' rights to either the company or the government.[43] This is key as companies often rely on third parties—such as protection unions or local authorities—to obstruct workers' organizing and bargaining efforts.

However, as illustrated by the Draxton case, authorities have been unable or reluctant to address potential violations committed by administrative bodies or courts through the RRM. Other cases in which likely administrative or judicial misconduct was an unresolved issue include *Grupo Yazaki*[44] and *Vidrio Decorativo Occidental*.[45] Thus, to reaffirm the Parties' intent to include administrative and judicial actions within the scope of the RRM, a clarification could be added to the agreement's text.

Systemic Improvements

1. Add a substantive obligation requiring all USMCA Parties to ensure employers bargain in good faith: While the RRM has been relatively successful in addressing freedom of association violations—such as securing the reinstatement of dozens of workers dismissed in retaliation for union activity—remediation related to collective bargaining has been far less common. Our analysis found that only in five cases were companies required to recognize and bargain with the petitioner union as part of the remediation process.

This gap in enforcement may stem from a perceived structural weakness in Mexican labor law. As previously discussed, unlike labor laws in the United States and Canada, Mexico's Federal Labor Law does not explicitly impose a legal obligation on employers to bargain in good faith. Although the newly established labor courts have begun to recognize the principle of bargaining in good faith, this has mostly occurred in cases where

[42] Traditionally, under international law, holding a State responsible for a violation requires linking the conduct to a State organ. Since the RRM focuses on what occurs at the facility level and its impact on workers' rights, attribution should not be a factor when determining whether a Denial of Rights has taken place. See "Article 4. Conduct of Organs of a State," in *Materials on the Responsibility of States for Internationally Wrongful Acts*, Book 25, Part One: Chapter II, United Nations Legislative Series (United Nations), accessed August 21, 2025, https://legal.un.org/legislativeseries/pdfs/chapters/book25/english/book25_part1_ch2_art4.pdf.

[43] USMCA Articles 31-A.2 and 31-B.2 state: "*The Mechanism shall apply whenever a Party (the 'complainant Party') has a good faith basis belief that workers at a Covered Facility are being denied the right of free association and collective bargaining under laws necessary to fulfill the obligations of the other Party (the 'respondent Party') under this Agreement (a 'Denial of Rights').*" If the Parties had intended the RRM to cover only Denials of Rights attributable to an enterprise, they would have stated so explicitly. Instead, the clause is written in the passive voice, recognizing that workers' rights can be denied by a range of actors. What matters under the agreement is the Denial of Rights itself, not the identity of the actor to whom the conduct could be attributed—whether a corporation, a protection union, or a local court.

[44] "Yazaki Case Summary," Maquila Solidarity Network, accessed February 7, 2025, https://www.maquilasolidarity.org/sites/default/files/resource/Yazaki-Case-Summary-MSN-Nov-2023.pdf.

[45] One of the allegations in the petition against Vidrio Decorativo Occidental concerned a local court's decision to declare a strike "non-existent" based on biased evidence submitted by the employer. In July 2024, a federal district court vacated that ruling. However, the company appealed, and the strike remained outlawed while an appeals tribunal considered the case. In the meantime, the U.S. government activated the mechanism but ultimately closed the case after the company carried out certain corrective actions—without restoring the workers' right to strike, which had been denied by the local court. As of this report's publication, the appeals tribunal has yet to issue a decision, leaving workers' right to strike effectively frustrated. The author's account of this case draws on firsthand experience as one of the petitioners.

an employer violated obligations under an existing CBA. As a result, enforcement efforts in Mexico—in the context of securing initial union contracts—rarely address employers' bargaining conduct or refusals to negotiate. Instead, labor authorities primarily focus on upholding the right to strike. Their role is limited to verifying the legality of a strike and, if confirmed, ensuring workers are supported in halting company operations.

While the right to strike is a core component of freedom of association, this right alone is not sufficient to guarantee meaningful collective bargaining. To better support workers' ability to secure union contracts, the USMCA should include an obligation for all Parties to require that employers bargain in good faith with unions that legally represent workers. A commitment to amend Mexico's Federal Labor Law to include this duty could be incorporated into Annex 23-A of the agreement.

2. Support efforts to grant sanctioning authority to Mexico's Federal Center for Labor Conciliation and Registration: While the RRM has been a groundbreaking tool for promoting labor law enforcement since Mexico's 2019 labor reform and the USMCA's entry into force in 2020, it cannot address all violations of freedom of association and collective bargaining across the country. Domestic authorities must also have the power to investigate and sanction violations. A bill granting the Federal Center sanctioning authority was approved by Mexico's lower congressional house in February 2024 but has stalled in the Senate. Amending Annex 23-A of the USMCA to require such authority under Mexican law would strengthen this legislative effort and expand labor rights enforcement nationwide.

3. Isolate fact-finding aspects of the RRM process and make it equally applicable to all USMCA Parties: If the RRM is to serve as a model for corporate accountability and fair competition tools in future trade agreements, it must evolve into a robust, independent, transparent, and reciprocal system.

In its current form, the RRM assigns dual roles to the U.S., Canadian, and Mexican governments: They are responsible for conducting factual investigations into petitions filed by unions and workers, while also participating in the international adjudication of disputes as competing parties. In the case of Mexico, this structure requires the government to simultaneously investigate complaints and defend companies accused of denying core labor rights—a dynamic that creates conflicting incentives and undermines the credibility of the Respondent's investigation.

Additionally, the system lacks transparency. Neither the Complainant nor the Respondent Party publishes or shares the outcomes of their investigations with relevant stakeholders. Companies under investigation do not have access to the original complaints, while unions and other petitioning groups are similarly unable to review the arguments or evidence submitted by the companies in their defense.

These limitations make a strong case for institutionalizing the RRM through the creation of an independent body tasked with investigating complaints and sharing findings with all stakeholders, including governments, unions, and employers. One of the few strengths of the NAFTA-era labor enforcement system was its production of

public reports, which helped raise awareness of labor rights challenges across the region.[46] A reformed RRM could build on this legacy of transparency while preserving its emphasis on company-specific remedies and rapid timelines.

Other relevant precedents for the evolution of the RRM include the 1999 U.S.–Cambodia Textile Agreement (UCTA) and the 2013 Accord on Fire and Building Safety in Bangladesh (Bangladesh Accord). The UCTA, in force from 1999 to 2004, linked Cambodian exporters' access to the U.S. apparel market to their compliance with national and international labor standards. Importantly, the governments enlisted the ILO to conduct facility-specific compliance monitoring, which added both credibility and transparency to the enforcement of the agreement. Throughout the duration of the agreement, the ILO published reports with aggregated data; however, when a factory failed to remedy identified violations, it also issued facility-specific reports to draw attention to the problems and force compliance.[47] Regarding the Bangladesh Accord, this private sector agreement was established in the aftermath of the 2013 Rana Plaza building collapse in Bangladesh, which killed more than 1,100 people and injured over 2,000. The tragedy starkly exposed the deplorable working conditions in much of the country's apparel industry. In response, the Accord created a system to improve factory safety standards. It proved highly successful, leading to inspections of more than 1,600 factories with over 90% of remediation works completed by 2018. For the purposes of this report, it is particularly relevant that the Accord relies on an independent Secretariat staffed with technical experts capable of impartially assessing compliance with safety standards. The Secretariat's assessments are fully transparent, and parties may challenge them through arbitration. To date, only two cases have reached arbitration, both resolved with substantial awards (including one of $2.3 million).[48] These experiences illustrate how either creating a new independent body or even enlisting the ILO to investigate facilities under the RRM—avoiding in this way duplicative investigations and conflicting incentives for the governments—is feasible and desirable to increase the transparency and credibility of the mechanism.

Finally, to ensure fairness and credibility, the RRM should be fully extended to cover facilities in the United States and Canada. This would ensure that workers in all three USMCA countries are equally protected and help prevent future distortions in labor standards and competition.

[46] "Submissions under the North American Agreement on Labor Cooperation (NAALC)," U.S. Department of Labor, Bureau of International Labor Affairs, accessed February 26, 2025, https://www.dol.gov/agencies/ilab/submissions-under-north-american-agreement-labor-cooperation-naalc.
[47] Sandra Polaski, "Combining Global and Local Forces: The Case of Labor Rights in Cambodia," *World Development* 34, no. 5 (May 2006), https://carnegie-production-assets.s3.amazonaws.com/static/files/WDCambodia1.pdf.
[48] "Bangladesh Accord Arbitration Cases—Resulting in Millions-of-Dollars in Settlements—Officially Closed," UNI Global Union, accessed August 22, 2025, https://uniglobalunion.org/news/bangladesh-accord-arbitration-cases-resulting-in-millions-of-dollars-in-settlements-officially-closed/.

Conclusion

The USMCA's Rapid Response Mechanism has marked a historic advancement in the integration of labor rights into trade enforcement. By delivering concrete wins for workers—particularly in addressing freedom of association violations in its initial years—it has demonstrated that trade agreements can serve as effective tools to promote corporate accountability and fair competition. However, the mechanism's long-term credibility and impact will depend on its continued evolution, including with critical improvements during the 2026 mandatory six-year USMCA review.

This report highlights several critical areas for reform. The growing reliance on "resolved during review" outcomes, the limited enforcement of collective bargaining rights, and the structural and transparency shortcomings of the current system all pose risks to the RRM's integrity. These challenges must be addressed through both procedural improvements, such as shortening the internal review period and revising panel request deadlines, and more systemic reforms, including mandating good faith bargaining obligations and institutionalizing independent, transparent investigation procedures.

Additionally, the RRM must become fully reciprocal and apply equally across all USMCA countries. Extending its scope to U.S. and Canadian facilities would not only ensure equal protections for workers throughout North America but also prevent distortions in competition rooted in uneven labor standards.

With certain legal and institutional changes, the RRM can be strengthened into a globally influential model for labor rights enforcement in trade. Its evolution into a more transparent, independent, and balanced mechanism is not only achievable—it is essential to deliver on the USMCA's promise of shared prosperity and respect for fundamental labor rights across the region.

Annex: List of RRM Petitions from Jul. 2020 to Jun. 2025

Case No.	Case Name	Date	Procedural requirements threshold	Request for Review
1	RRM Petition - 2021-01 (Mexico) vs. Mexico City Firefighters	2/16/21	Failed	NA
2	RRM Petition - 2021-02 (Mexico) vs. Mexican Airspace Navigation Services (Air Traffic controllers)	3/2/21	Failed	NA
3	RRM Petition - 2021-03 (Mexico) vs. Tridonex	5/10/21	Passed	Yes
4	RRM Petition - 2021-04 (Mexico) vs. General Motors Silao	5/12/21	NA – Self-initiated	Yes
5	RRM Petition - 2021-05 (Mexico) vs. Hard Rock Hotels	7/15/21	Failed	NA
6	RRM Petition - 2021-06 (Mexico) vs. Chiapas University	8/5/21	Failed	NA
7	RRM Petition - 2022-01 (Mexico) vs. Panasonic	4/18/22	Passed	Yes
8	RRM Petition - 2022-02 (Mexico) vs. Teksid	5/5/22	Passed	Yes
9	RRM Petition - 2022-03 (Mexico) vs. VU Manufacturas	6/21/22	Passed	Yes
10	RRM Petition - 2022-04 (Mexico) vs. BBB	8/2/22	Passed	No
11	RRM Petition - 2022-05 (Mexico) vs. St. Gobain	9/27/22	Passed	No
12	RRM Petition - 2022-06 (Mexico) vs. VU Manufacturas 2.0	12/29/22	Passed	Yes
13	RRM Petition - 2023-01 (Mexico) vs. Unique Fabricating	2/2/23	Passed	Yes
14	RRM Petition - 2023-02 (Mexico) vs. Goodyear	4/20/23	Passed	Yes
15	RRM Petition - 2023-03 (Mexico) vs. INISA	5/12/23	Passed	Yes
16	RRM Petition - 2023-04 (Mexico) vs. San Martin	5/15/23	Passed	Yes
17	RRM Petition - 2023-05 (Mexico) vs. Home Depot	5/25/23	Failed	NA

Case No.	Case Name	Date	Procedural requirements threshold	Request for Review
18	RRM Petition - 2023-06 (Mexico) vs. Draxton	2/16/21	NA – Self-initiated	Yes
19	RRM Petition - 2023-07 (Mexico) vs. Yazaki	3/2/21	Passed	Yes
20	RRM Petition - 2023-08 (Mexico) vs. CEMEX (Tugboat)	7/21/23	Passed	No
21	RRM Petition - 2023-09 (Mexico) vs. MASAIR (Pilots)	7/31/23	Passed	Yes
22	RRM Petition - 2023-10 (Mexico) vs. TEKLAS	8/24/23	Passed	Yes
23	RRM Petition - 2023-11 (Mexico) vs. Asiaway	9/20/23	Passed	Yes
24	RRM Petition - 2023-12 (Mexico) vs. Tecnologia Modificada (Caterpillar)	9/25/23	Passed	Yes
25	RRM Petition - 2023-13 (Mexico) vs. Autoliv	10/19/23	Passed	Yes
26	RRM Petition - 2023-14 (Mexico) vs. Fujikura	11/13/23	Passed	Yes
27	RRM Petition - 2023-15 (Mexico) vs. Atento Call Center	12/18/23	Passed	Yes
28	RRM Petition - 2024-01 (Mexico) vs. RV Fresh Foods	1/17/24	Passed	Yes
29	RRM Petition - 2024-02 (Mexico) vs. SIG	2/29/24	Passed	Yes
30	RRM Petition - 2024-03 (Mexico) vs. Patron Spirits	2/29/24	Passed	No
31	RRM Petition - 2024-04 (Mexico) vs. Tizapa	3/4/24	Passed	Yes
32	RRM Petition - 2024-05 (Mexico) vs. Pemex Hospital	4/17/24	Failed	NA
33	RRM Petition - 2024-06 (Mexico) vs. Tin Izzi	4/23/24	Failed	NA
34	RRM Petition - 2024-07 (Mexico) vs. VW Puebla	4/25/24	Passed	Yes

Case No.	Case Name	Date	Procedural requirements threshold	Request for Review
35	RRM Petition - 2024-08 (Mexico) vs. Industrias Tecnos	5/23/24	Passed	Yes
36	RRM Petition - 2024-09 (Mexico) vs. Tecnologia Modificada (Caterpillar) 2.0	5/28/24	Passed	No
37	RRM Petition - 2024-10 (Mexico) vs. IMPRO Industries	6/24/24	Passed	Yes
38	RRM Petition - 2024-11 (Mexico) vs. Camino Rojo Mine	6/24/24	Passed	Yes
39	RRM Petition - 2024-12 (Mexico) vs. Yamaha	7/23/24	Passed	No
40	RRM Petition - 2024-13 (Mexico) vs. Pirelli	7/23/24	Passed	Yes
41	RRM Petition - 2024-14 (Mexico) vs. Bader	8/15/24	Passed	Yes
42	RRM Petition - 2024-15 (Mexico) vs. ODISA	9/23/24	Passed	Yes
43	RRM Petition - 2024-16 (Mexico) vs. Dasung	9/24/24	Passed	No
44	RRM Petition - 2024-17 (Mexico) vs. Vidrio Decorativo Occidental	10/10/24	Passed	Yes
45	RRM Petition 2024-18 (Mexico) vs. Contitech	10/21/24	Passed	No
46	RRM Petition 2024-19 (Mexico) vs. Tizapa Mine 2.0	10/23/24	Passed	No
47	RRM Petition 2024-20 (Mexico) vs. Akwel	10/24/24	Passed	Yes
48	RRM Petition 2024-21 (Mexico) vs. Tornel	12/9/24	Passed	Yes
49	RRM Petition 2025-01 (Mexico) vs. Autotransportes Varela	NA	Withdrawn	NA
50	RRM Petition 2025-02 (Mexico) vs. Aludyne	3/3/25	Passed	Yes
51	RRM Petition 2025-03 (Mexico) vs. Modern Metal Alloys	3/17/25	Passed	Yes
52	RRM Petition 2025-04 (Mexico) vs Tizapa Mine 3.0	3/26/25	Failed	NA

Case No.	Case Name	Date	Procedural requirements threshold	Request for Review
53	RRM Petition 2025-05 (Mexico) vs Amphenol Optimize México	4/11/25	Passed	Yes
54	RRM Petition 2025-06 (Mexico) vs Mondelez México	4/30/25	Passed	No
55	RRM Petition 2025-07 (Mexico) v. Superior	5/5/25	Passed	Yes
56	RRM Petition 2025-08 (Mexico) v. Linamar	5/12/25	Passed	No
57	RRM Petition 2025-09 (Mexico) v. TAMSA	5/15/25	Passed	Yes
58	RRM Petition 2025-10 (Mexico) v. Liber Gennesys	6/12/25	Passed	Yes

The American Economic Liberties Project is a non-profit and non-partisan organization fighting against concentrated corporate power to secure economic liberty for all. We do not accept funding from corporations. Contributions from foundations and individuals pay for the work we do.

Rethink Trade was established to intensify analysis and advocacy regarding the myriad ways that today's trade agreements and policies must be altered to undo decades of corporate capture and to deliver on broad public interests including resilient supply chains and fair markets, the creation and support of good jobs with workers empowered to earn decent wages, public health and safety delivered by strong consumer and environmental protections, and the ability for those who will live with the results to decide the policies affecting their lives.

economicliberties.us
@econliberties
info@economicliberties.us

rethintrade.org
@rethinktrade
info@rethinktrade.org

International Preemption by "Trade" Agreement: Big Tech's Ploy to Undermine Privacy, AI Accountability, and Anti-Monopoly Policies"

March 2023

Daniel Rangel
Lori Wallach

About the Authors

Daniel Rangel is the research director of the Rethink Trade program at Economic Liberties. Daniel specializes in international trade and investment law and policy and he is an expert in trade and labor matters. He was one of the lawyers that drafted the first stakeholder petition to activate the USMCA rapid response mechanism.

Lori Wallach is the director of the Rethink Trade program at Economic Liberties and a 30-year veteran of international and U.S. congressional trade battles. She was named to "Politico's 50" list of thinkers, doers and visionaries transforming American politics for her leadership in the Trans-Pacific Partnership (TPP) debate. A lawyer, Lori is the author of The Rise and Fall of Fast Track Trade Authority and Whose Trade Organization? A Comprehensive Guide to the WTO.

Introduction

The 117th Congress featured an unprecedented array of bills aimed at reining in the Big Tech giants that dominate global retail, advertising, transportation, and other sectors. Legislation that would end or mitigate big platforms' abuses of workers, consumers, and smaller businesses was approved by committees. Lawmakers sought to counter online commercial surveillance and the exploitation of U.S. citizens' personal data, to ensure that artificial intelligence (AI) systems do not mask discrimination or deliver inaccurate outcomes, and to level the playing field for smaller actors in digital markets. Most of these legislative proposals did not become law thanks to Big Tech lobbying. However, many of the bills will be reintroduced in the new Congress and support for regulating the digital economy is only growing.

One powerful, if stealthy, strategy Big Tech is prioritizing to derail these efforts is a form of international preemption. The goal is to excavate the policy space out from under Congress and the administration by locking the United States and its trade partners into international rules that forbid such digital governance initiatives. The goal is to secure binding international "digital trade" rules that limit, if not outright forbid, governments from enacting or enforcing domestic policies to counter Big Tech privacy abuses and online surveillance, AI discrimination, and other threats and monopolistic misconduct that threaten our economy and democracy.

This is not a hypothetical threat. Special interests have rigged past trade pacts to achieve unpopular agendas unrelated to trade. For instance, 1990s trade agreements included rules requiring the United States to extend drug patents from 17-year to 20-year monopoly terms after Big Pharma was unable to win this price-boosting change in Congress after decades of trying via regular order.[1]

Today, Big Tech lobbyists are trying to exploit closed-door trade-negotiating processes and arcane trade terminology by pushing on many fronts for "digital trade" rules to handcuff Congress and regulators. This includes Indo-Pacific Economic Framework (IPEF) negotiations, U.S.-EU Trade and Technology Council (TTC) talks, and possible Americas Partnership for Economic Prosperity (APEP) talks. The terms being formulated for these secretive talks not only conflict with congressional proposals but the administration's Blueprint for an AI Bill of Rights[2] and its Executive Order 14036/2021 on Promoting

1 See, e.g., Schondelmeyer SW, "Economic Impact of GATT Patent Extension on Currently Marketed Drugs," PRIME Institute, College of Pharmacy, University of Minnesota 1995; and Jorge MF, "Tough medicine: Ensuring access to affordable drugs requires fixing trade agreements starting with NAFTA," Journal of Generic Medicines. 2018. Available at 10.1177/1741134318810061.

2 The White House, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People. October 2022. Available at: https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

Competition in the American Economy.[3] If this strategy succeeds, rules shielding Big Tech abuses would be imposed via the backdoor of "trade pacts" here and in countries comprising much of the world economy, even as public and policymaker anger about Big Tech excesses grows across partisan divides.

This policy brief uses excerpts from 117th Congress bills and from administration policy documents to show the direct conflicts between prominent U.S. domestic digital governance proposals and the "digital trade" agenda that Big Tech interests seek in current trade negotiations. The Trump administration included a pro-Big-Tech Digital Trade chapter in the U.S.-Mexico-Canada Agreement (USMCA). USMCA Chapter 19 expands on what was viewed as a Big Tech-rigged Electronic Commerce chapter in the Trans-Pacific Partnership (TPP). Many of the restrictions on domestic policy in USMCA Chapter 19 are not found in other nations' pacts that have digital terms. Big Tech interests have been clear that their goal is, at a minimum, to replicate the USMCA/TPP approach to "digital trade" rules in current trade talks, and with respect to some sensitive issues push for broader prerogatives for tech firms and new limits on governments.[4]

Key USMCA "digital trade" terms conflict with digital governance initiatives here and abroad. For instance, even as President Biden has repeatedly declared that the expansive liability shield for tech platforms provided by Section 230 of the Communications Decency Act must be altered[5] and members of Congress from across the political spectrum agree, the USMCA text requires countries to adopt and enforce that very policy. **In this policy brief, we examine three of the most invasive provisions from the USMCA "digital trade" chapter that conflict with U.S. policy initiatives and that Big Tech interests seek to include in the IPEF and other pacts now being negotiated**. These include:

- **New Secrecy Guarantees that Forbid Screening of Algorithms and Code for Racial Bias, Labor Law Violations, or Other Abuses – USMCA Article 19.16 (Source Code):** In conflict with core concepts in the administration's Blueprint for an AI Bill of Rights, the American Data Privacy and Protection Act's rules on civil rights and algorithms, and the Facial Recognition Act of 2022's testing requirements, among other policies, this term would ban governments from prescreening or conducting general reviews of AI code or algorithms for racial and other forms of discrimination, labor law or competition policy violations, biases in criminal justice applications, and more.

3 Federal Register, Executive Order 14036 of July 9, 2021, Promoting Competition in the American Economy. Available at: https://www.federalregister.gov/documents/2021/07/14/2021-15069/promoting-competition-in-the-american-economy.

4 See U.S. Chamber of Commerce, The Digital Trade Revolution. p. 16. Available at: https://www.uschamber.com/assets/documents/Final-The-Digital-Trade-Revolution-February-2022_2022-02-09-202447_wovt.pdf; Christine Bliss, Coalition of Services Industries, Testimony, Senate Finance Subcommittee on International Trade, Wed. Nov. 30, 2022. Available at: uschamber.com/international/trade-agreements/the-digital-trade-revolution-how-u-s-workers-and-companies-can-benefit-from-a-digital-trade-agreement

5 Joe Biden, "Republicans and Democrats, Unite Against Big Tech Abuses," Wall Street Journal, Jan. 11, 2023. Available at https://www.wsj.com/articles/unite-against-big-tech-abuses-social-media-privacy-competition-antitrust-children-algorithm-11673439411; The White House, "Readout of White House Listening Session on Tech Platform Accountability," Sept. 8, 2022. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/08/readout-of-white-house-listening-session-on-tech-platform-accountability/.

- **Forbidding Limits on Firms' Control of Data, Including Rights to Move, Process, and Store Personal Data Wherever the Firms Choose – USMCA Article 19.11 (Cross-Border Transfer of Information by Electronic Means) and Article 19.12 (Location of Computing Facilities):** The goals and core terms of policies like the American Data Privacy and Protection Act and My Body, My Data Act of 2022, or similar legislation, could be undermined if firms can evade obligations to eliminate private data according to users' requests or minimize collection by transferring it to another firm in a jurisdiction where U.S. law enforcement cannot reach – and no similar protections are available to consumers – or if, for instance, an offshore processor is able to sell data onward to another firm that is located in a country where no protections apply. These terms would also undermine efforts to regulate the data brokerage industry.
- **Designation of Key Anti-Monopoly Policies as Discriminatory Illegal Trade Barriers – USMCA Article 19.4 (Non-Discriminatory Treatment of Digital Products):** This broad USMCA provision brands policies that treat foreign and domestic firms the same, but have a greater impact on bigger firms, as illegal trade barriers that must be eliminated. Currently, this USMCA language is being used by tech industry lobbyists to attack a Canadian initiative that is similar to the U.S. Journalism Competition and Preservation Act. The concept underlying this clause has also been used to attack an equivalent Australian law; South Korea's app store legislation, which resembles the Open App Markets Act in the United States; and the EU's Digital Markets Act, which shares some elements with the American Innovation and Choice Online Act.

The lack of U.S. domestic digital governance policy makes the threat posed by international preemption via "digital trade" rules set in international trade negotiations particularly dangerous. Congress has not established national privacy or data safety protections or created policies to ensure that AI uses do not undermine civil, labor, and other rights or set parameters to ensure fair digital markets. That means that negotiators effectively are making the U.S. law as they negotiate the international rules, rather than being guided by domestic policies already established by Congress. Given trade negotiations occur behind closed doors and almost all of the 500 official U.S. trade advisors represent corporate interests, it is not surprising that past "digital trade" rules found in the USMCA and the TPP are so direly lopsided in Big Tech's favor. As Congress and executive branch regulatory agencies now push to create a U.S. digital governance regime, the approach to any digital terms in trade agreements must be reconsidered and significantly altered.

I. Extreme Algorithmic and Source Code Secrecy Rules

The development of artificial intelligence technologies, the evolution of the internet, and the growth of the data economy are fundamentally transforming every aspect of our lives. AI technologies can lead to more efficient exchanges and decision making. Yet unchecked and unregulated use of AI, sometimes also called automated systems, has proven harmful: It enables discriminatory policing, prosecution, and housing and job

recruitment; intrusive worker surveillance; and unfair lending practices.

Examples of real and potential damage to people, particularly minorities, from unregulated use of AI abound. The National Institute of Standards and Technology found that facial recognition technologies driven by 189 different algorithms were least accurate on women of color.[6] San Francisco, Boston, and other cities have banned the technology's use by police after decades of negative consequences for people of color.[7] Yet in much of the country, such technologies remain in use.

Wide use of automated decision systems in consumer finance is likely to be entrenching or even worsening the long-standing discrimination that minorities face in credit markets. A 2021 study discovered that lenders were 40 to 90% more likely to turn down Latino, Asian, Native American, and Black applicants than similar white applicants. Black applicants in higher income brackets with less debt were rejected more often than white applicants in the same income bracket who had more debt.[8] Housing and employment websites driven by AI are rife with discrimination. For instance, Facebook was recently accused of algorithmic discrimination in job advertising before the Equal Employment Opportunity Commission.[9] A female truckers association claims Facebook selectively shows job ads based on users' gender and age, with older workers and women far less likely to see ads for blue-collar positions, especially in industries that have historically excluded women.[10]

Another problematic venue for AI use is the criminal justice system, where AI risk assessments are used to set defendants' bail,[11] judge eligibility for alternative rehabilitative treatment,[12] determine conditions of probation[13] and – in some states – set sentencing and duration of prison time for defendants![14] Yet, these tools rely on algorithms that are potentially fed biased and inaccurate data. AI-enabled digital technologies also are being used by employers to recruit, hire, and evaluate the performance of and exert control over workers.

Unchecked and unregulated usage of AI technologies by employers can easily lead to violations of wage and hour labor laws with work speed-ups and scheduling gimmicks. In

6 Patrick Grother, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, Nat'l Institute of Standards and Technology, Dec. 2019. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

7 Alex Najibi, Racial Discrimination in Face Recognition Technology, Science Policy and Social Justice, Harvard Univ., Oct. 24, 2020. Available at: https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

8 Emmanuel Martinez et al., "The Secret Bias Hidden in Mortgage-Approval Algorithms," The Markup, Aug. 2021. Available at: https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

9 Alexia Fernández Campbell, "Job ads on Facebook discriminated against women and older workers, EEOC says," Vox, Sept. 25, 2019. Available at https://www.vox.com/identities/2019/9/25/20883446/facebook-job-ads-discrimination.

10 Jessica Guynn, "Are Facebook job ads discriminatory? Company accused of bias against women, older workers," USA Today, Dec. 1, 2022. Available at: https://www.usatoday.com/story/money/2022/12/01/facebook-jobs-ads-discrimination-women-older-workers/10810589002/.

11 Anna Maria Barry-Jester et al., "The New Science of Sentencing," The Marshall Project, Aug. 2015. Available at: https://www.themarshallproject.org/2015/08/04/the-new-science-of-sentencing.

12 Julia Angwin et al., "Machine Bias," ProPublica, May 23, 2016. Available at: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. See also Kate Crawford, "Artificial Intelligence's White Guy Problem," New York Times, June 26, 2016. Available at: https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html?mcubz=1.

13 Eileen Sullivan et al., "States predict inmates' future crimes with secretive surveys," Associated Press, February 2015. Available at: https://apnews.com/article/027a00d70782476eb7cd07fbcca40fc2.

14 Alexandra Chouldekova, "Fair Prediction with Disparate Impact: A Study of Bias in Recidivism Prediction Instruments," (Updated February 2017). Available at: https://arxiv.org/pdf/1703.00056.pdf.

2015, workers filed class-action lawsuits against McDonald's stores in California, Michigan, and New York, alleging systematic wage theft associated with workplace management software. The stores involved reportedly used a computer program to calculate labor costs every 15 minutes as a percentage of revenue. When labor costs were above a predetermined target, managers ordered employees to clock out and wait in break rooms for minutes or hours without pay and only clock back in when revenue increased. Managers would tell workers to clock out before their shifts ended but insist they finish certain tasks before going home.[15]

Congressional committees, scholars, journalists, and government investigators have tried to review AI applications' source code and related datasets to identify racist, sexist, and other practices deserving of scrutiny, criticism, and correction. Many U.S. agencies and courts require access to source code to perform essential government functions related to tax collection, financial transaction oversight, car safety, and even gambling regulation.[16] More importantly, U.S. policymakers are responding to a growing movement for AI accountability or transparency and algorithmic justice. The goal is for governments to have the tools to not only sanction, but prevent, discriminatory or abusive practices. Experts have recommended enacting policies that enable effective external audits of AI systems and require governmental pre-market authorization conditioned upon access to source code for high-risk sectors like access to health services, credit scoring, education, or employment opportunities.[17] Color of Change's "Black Tech Agenda" lists many of the bills that aim to address these threats and calls for such prescreening, particularly of AI deployed in sensitive sectors relating to criminal justice and access to health care, credit, and employment opportunities.[18]

In October 2022, the White House released "The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People." This document is intended to support the development of policies and practices to protect civil rights and promote democratic values in the building, use, and governance of artificial intelligence. The blueprint also calls for pre-deployment testing, risk identification and mitigation, and ongoing monitoring to ensure that AI systems are not unsafe, discriminatory, or inaccurate, which should be confirmed by independent evaluation via algorithmic impact assessments.[19]

While a broad array of proposals rely on regulators being able to prescreen AI to ensure AI programs are not abused for illegal police surveillance or denial of credit or otherwise violate Americans' civil rights and liberties, USMCA and TPP include broad restrictions on

15 Esther Kaplan, "The Spy Who Fired Me," Harper's Magazine, Mar. 2015. Available at: https://harpers.org/archive/2015/03/the-spy-who-fired-me/.

16 "Some preliminary implications of WTO source code proposal," Briefing, Dec. 2017. Available at: https://www.twn.my/MC11/briefings/BP4.pdf

17 Data Ethics Commission, "Opinion of the Data Ethics Commission," p. 19, 2019. Available at: https://www.bmj.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN.pdf?__blob=publicationFile&v=2; Kristina Irion, "AI regulation in the EU and Trade Law: How Can Accountability of AI and a High Level of Consumer Protection Prevail over a Trade Discipline on Source Code?" p. 25-26, Jan. 26, 2021. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3786567.

18 Color of Change, The Black Tech Agenda, 2022. Available at: https://blacktechagenda.org/.

19 Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People, White House, Office of Science and Technology Policy, Oct. 2022. Available at: https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

regulators' access to sources code and algorithms. Until TPP and USMCA, U.S. pacts did not include these extreme terms. Such prohibitions also are not included in other nations' digital agreements. Only 11 of the 181 agreements with digital trade or e-commerce terms include the extreme secrecy guarantees for source code in USMCA and TPP, which forbid governments from routinely prescreening source code and algorithms for racial discrimination or other law violations.[20]

Notably, the USMCA prohibition is especially expansive. It covers "*a source code of software (…)*," which is also covered in the TPP, but also "*an algorithm expressed in that source code*." The USMCA Article 19.1 defines algorithm as: "a defined sequence of steps, taken to solve a problem or obtain a result." USMCA's source code provision then encompasses not only the source code, but the sequence of steps to solve a problem or obtain a result. This means that the USMCA disclosure prohibition potentially covers descriptions of algorithms, not only the detailed source code developed by programmers. This problematic, broad obligation could then preclude even the less expansive prescreening requirements included in some legislative proposals that mandate disclosing to the authorities detailed descriptions of algorithms' design process and methodologies. For instance, consider the American Data Privacy and Protection Act (ADPPA), which was approved by a large bipartisan majority of the House Committee on Energy and Commerce in July 2022 and is likely to be reintroduced this Congress.[21] If it becomes law in the 118th Congress, it would be the first U.S. national policy protecting personal data. The ADPPA includes a "civil rights and algorithms" provision, which requires certain entities to submit impact assessments and algorithm design evaluations to the Federal Trade Commission.[22] Even such descriptive impact assessments and design evaluations would be ensnared by the expansive USMCA definition of information that governments are barred from accessing.

The chart on the following page displays the relevant USMCA article that includes the extreme source code and algorithm secrecy guarantees and the provisions of the ADPPA and other federal bills promoting AI accountability, along with excerpts from the Biden administration's AI Bill of Rights, which would be undermined by Big Tech's "digital trade" agenda.

20 Calculations made using the TAPED dataset, "The Governance of Big Data in Trade Agreements," Universities of Lucerne and Bern. Accessed on Oct. 3, 2022. Available at: https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/research/taped/.

21 Aysha F. Allos, "American Data Privacy and Protection Act: Are We Finally Getting Federal Data Privacy Protection?" The National Law Review, Sept. 21 2022. Available at: https://www.natlawreview.com/article/american-data-privacy-and-protection-act-are-we-finally-getting-federal-data-privacy.

22 Section 207(c) of the American Data Privacy and Protection Act. Accessed on Sept. 25, 2022. Available at: https://www.congress.gov/bill/117th-congress/house-bill/8152/text#toc-H6332551148B14109B1F2D9598E099E38.

USMCA Article 19.16: Source Code

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. *[Emphasis added]*

[6] This disclosure shall 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.

Threatened Domestic Policy Initiatives	Provisions
American Data Privacy and Protection Act (H.R.8152) Sponsor: Rep. Frank Pallone Jr. (D-NJ). Cosponsors: Rep. Cathy McMorris Rodgers (R-WA), Rep. Janice Schakowsky (D-IL), and Rep. Gus Bilirakis (R-FL). *[Senate Commerce Committee Ranking Member Sen. Roger Wicker (R-MS) also backs the bill.]*	**SEC. 207. CIVIL RIGHTS AND ALGORITHMS.** (...) (c) ALGORITHM IMPACT AND EVALUATION.— (1) ALGORITHM IMPACT ASSESSMENT.— (A) IMPACT ASSESSMENT.—Notwithstanding any other provision of law, not later than 2 years after the date of enactment of this Act, and annually thereafter, a large data holder that uses an algorithm that may cause potential harm to an individual, and uses such algorithm solely or in part, to collect, process, or transfer covered data must conduct an impact assessment of such algorithm in accordance with subparagraph (B). (B) IMPACT ASSESSMENT SCOPE.—The impact assessment required under subparagraph (A) shall provide the following: (i) A detailed description of the design process and methodologies of the algorithm. (ii) A statement of the purpose, proposed uses, and foreseeable capabilities outside of the articulated proposed use of the algorithm. (iii) A detailed description of the data used by the algorithm, including the specific categories of data that will be processed as input and any data used to train the model that the algorithm relies on. (iv) A description of the outputs produced by the algorithm. (v) An assessment of the necessity and proportionality of the algorithm in relation to its stated purpose, including reasons for the superiority of the algorithm over nonautomated decision-making methods. (...) (2) ALGORITHM DESIGN EVALUATION.—Notwithstanding any other provision of law, not later than 2 years after the date of enactment of this Act, a covered entity or service provider that knowingly develops an algorithm, solely or in part, to collect, process, or transfer covered data or publicly available information shall prior to deploying the algorithm in interstate commerce evaluate the design, structure, and inputs of the algorithm, including any training data used to develop the algorithm, to reduce the risk of the potential harms identified under paragraph (1)(B). (3) OTHER CONSIDERATIONS.— (...)

	(B) EXTERNAL, INDEPENDENT AUDITOR OR RESEARCHER.—To the extent possible, a covered entity and a service provider shall utilize an external, independent auditor or researcher to conduct an impact assessment under paragraph (1) or an evaluation under paragraph (2). (C) AVAILABILITY.— (i) IN GENERAL.—A covered entity and a service provider— (I) shall, not later than 30 days after completing an impact assessment or evaluation, submit the impact assessment and evaluation conducted under paragraphs (1) and (2) to the Commission; (II) shall, upon request, make such impact assessment and evaluation available to Congress; (...) (ii) TRADE SECRETS.—Covered entities and service providers must make all submissions under this section to the Commission in unredacted form, but a covered entity and a service provider may redact and segregate any trade secrets (as defined in section 1839 of title 18, United States Code) from public disclosure under this subparagraph. *[Emphasis added]*
Facial Recognition Act of 2022 (H.R.9061) Sponsor: Rep. Ted Lieu (D-CA). Cosponsors: Rep. Sheila Jackson Lee (D-TX), Rep. Yvette Clarke (D-NY), and Rep. Jimmy Gomez (D-CA).	SEC. 106. ACCURACY AND BIAS TESTING. (a) Benchmark Testing.—No investigative or law enforcement officers may use a facial recognition system or information derived from it unless that system is annually submitted to the National Institute of Standards and Technology's benchmark facial recognition test for law enforcement to determine— (1) the accuracy of the system; and (2) whether the accuracy of the system varies significantly on the basis of race, ethnicity, gender or age. (b) Benchmark Testing For New Systems.—No investigative or law enforcement officers may begin using a new facial recognition system or information derived from it unless that system is first submitted to independent testing to determine— (1) the accuracy of the system; and (2) whether the accuracy of the system varies significantly on the basis of race, ethnicity, gender, or age. (c) Prohibition.—Any investigative or law enforcement officer may not use facial recognition that has not achieved a sufficiently high level of accuracy, including in terms of overall accuracy and variance on the basis of race, ethnicity, gender, or age, as determined by the National Institute of Standards and Technology, on its annual benchmark test for law enforcement use. (d) Operational Testing.—No investigative or law enforcement agencies may use a facial recognition system or information derived from it unless that system is annually submitted to operational testing conducted by an independent entity, in accordance with National Institute of Standards and Technology's training protocol for operational testing, to determine— (1) the accuracy of the system; (2) the impact of human reviewers on system accuracy; and (3) whether the accuracy of the system varies significantly on the basis of race, ethnicity, gender, or age. (...)

	SEC. 201. NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY ASSISTANCE. (a) In General.—The National Institute of Standards and Technology (hereinafter in this section referred to as "NIST") shall— (1) develop best practices for law enforcement agencies to evaluate the accuracy and fairness of their facial recognition systems; (2) develop and offer an ongoing benchmark facial recognition test for law enforcement that— (A) conducts evaluations of actual algorithms used by law enforcement agencies; (B) uses the types of probe images, including in terms of quality, actually used by law enforcement agencies in its testing; (C) evaluates algorithms on larger databases that reflect the size of databases actually used by law enforcement; and (D) evaluates whether the accuracy of a facial recognition algorithm varies on the basis of race, ethnicity, gender, or age and assessments of bias in facial recognition systems; (3) develop an operational testing protocol that independent testers and law enforcement agencies may implement for annual operational testing to determine— (A) the accuracy of the facial recognition system; (B) the impact of human reviewers on facial recognition system accuracy; and (C) whether the accuracy of the facial recognition system varies significantly on the basis of race, ethnicity, gender, or age; and (4) study and develop training standards for human operators reviewing the results of facial recognition searches to ensure accuracy and prevent bias. *[Emphasis added]*
Justice in Forensic Algorithms Act of 2021 (H.R.2438) Sponsor: Rep. Mark Takano (D-CA). Cosponsor: Rep. Dwight Evans (D-PA).	SEC. 2. COMPUTATIONAL FORENSIC ALGORITHM TESTING STANDARDS. (c) Requirements For Federal Use Of Forensic Algorithms.—Any Federal law enforcement agency or crime laboratory providing services to a Federal law enforcement agency using computational forensic software may use only software that has been tested under the National Institute of Standards and Technology's Computational Forensic Algorithm Testing Program and shall conduct an internal validation according to the requirements outlined in the Computational Forensic Algorithm Testing Standards and make the results publicly available. The internal validation shall be updated when there is a material change in the software that triggers a retesting by the Computational Forensic Algorithm Testing Program. (...) (f) Use Of Computational Forensic Software.—Any results or reports resulting from analysis by computational forensic software shall be provided to the defendant, and the defendant shall be accorded access to both an executable copy of and the source code for the version of the computational forensic software—as well as earlier versions of the software, necessary instructions for use and interpretation of the results, and relevant files and data—used for analysis in the case and suitable for testing purposes. *[Emphasis added]*

Facial Recognition and Biometric Technology Moratorium Act of 2021 (H.R.3907/S.2052) Sponsors: Rep. Pramila Jayapal (D-WA) and Sen. Edward Markey (D-MA). Cosponsors: Rep. Ayanna Pressley (D-MA), Rep. Rashida Tlaib (D-MI), Rep. Anna Eshoo (D-CA), Rep. Adriano Espaillat (D-NY), Del. Eleanor Holmes Norton (D-DC), Rep. Ilhan Omar (D-MN), Rep. Bobby Rush (D-IL), Rep. Earl Blumenauer (D-OR), Rep. Alan Lowenthal (D-CA), Rep. Mark DeSaulnier (D-CA), Rep. Judy Chu (D-CA), Rep. Cori Bush (D-MO), Rep. Yvette Clarke (D-NY), Rep. Jamie Raskin (D-MD), Rep. Andre Carson (D-IN), Rep. Janice Schakowsky	SEC. 3. PROHIBITION ON FEDERAL GOVERNMENT USE OF BIOMETRIC SURVEILLANCE. (a) In General.—Except as provided in subsection (b), it shall be unlawful for any Federal agency or Federal official, in an official capacity, to acquire, possess, access, or use in the United States— (1) any biometric surveillance system; or (2) information derived from a biometric surveillance system operated by another entity. (b) Exception.—The prohibition set forth in subsection (a) does not apply to activities explicitly authorized by an Act of Congress that describes, with particularity— (1) the entities permitted to use the biometric surveillance system, the specific type of biometric authorized, the purposes for such use, and any prohibited uses; (2) standards for use and management of information derived from the biometric surveillance system, including data retention, sharing, access, and audit trails; (3) auditing requirements to ensure the accuracy of biometric surveillance system technologies, standards for minimum accuracy rates, and accuracy rates by gender, skin color, and age; (4) rigorous protections for due process, privacy, free speech and association, and racial, gender, and religious equity; and (5) mechanisms to ensure compliance with the provisions of the Act. *[Emphasis added]*

(D-IL), Sen. Jeff Merkley (D-OR), Sen. Bernard Sanders (I-VT), Sen. Elizabeth Warren (D-MA), Sen. Ron Wyden (D-OR), and Sen. Cory Booker (D-NJ).	
Platform Accountability and Transparency Act (S.5339) Sponsor: Sen. Christopher Coons (D-DE). Cosponsors: Sen. Rob Portman (R-OH), Sen. Amy Klobuchar (D-MN), and Sen. Bill Cassidy (R-LA).	SEC. 2. DEFINITIONS. In this Act: (...) (6) QUALIFIED DATA AND INFORMATION.— (A) IN GENERAL.—Subject to subparagraph (B), the term "qualified data and information" means data and information from a platform— (i) that the NSF determines is necessary to allow a qualified researcher to carry out a qualified research project; and (ii) that— (I) is feasible for the platform to provide; (II) is proportionate to the needs of the qualified researchers to complete the qualified research project; (III) will not cause the platform undue burden in providing the data and information to the qualified researcher; and (IV) would not be otherwise available to the qualified researcher. (B) EXCLUSIONS.—Such term does not include any of the following: (i) Direct and private messages between users. (ii) Biometric information, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics. (iii) Precise geospatial information. (...) SEC. 4. OBLIGATIONS AND IMMUNITY FOR PLATFORMS. (a) Provision Of Qualified Data And Information.—A platform shall provide access to qualified data and information relating to a qualified research project to a qualified researcher under the terms and privacy and cybersecurity safeguards dictated by the Commission for the purpose of carrying out the qualified research project.

	(e) Right Of Review.—If a platform fails to provide all of the qualified data and information required under the terms of a qualified research project to the qualified researcher conducting the project, the qualified researcher or the researcher's affiliated university or nonprofit organization may bring an action in district court for injunctive relief or petition the Commission *[FTC]* to bring an enforcement action against the platform. SEC. 7. ENFORCEMENT. (a) Unfair Or Deceptive Act Or Practice.— (1) IN GENERAL.—A platform's failure to comply with subsection (a) or (b) of section 4, or a qualified researcher's failure to comply with subsection (a) or (b) of section 5, shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)). *[Emphasis added]*
White House Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People	SAFE AND EFFECTIVE SYSTEMS **You should be protected from unsafe or ineffective systems.** Automated systems should be developed with consultation from diverse communities, stakeholders, and domain experts to identify concerns, risks, and potential impacts of the system. Systems should undergo pre-deployment testing, risk identification and mitigation, and ongoing monitoring that demonstrate they are safe and effective based on their intended use, mitigation of unsafe outcomes including those beyond the intended use, and adherence to domain-specific standards. (…) Independent evaluation and reporting that confirms that the system is safe and effective, including reporting of steps taken to mitigate potential harms, should be performed and the results made public whenever possible. ALGORITHMIC DISCRIMINATION PROTECTIONS **You should not face discrimination by algorithms and systems should be used and designed in an equitable way**. Algorithmic discrimination occurs when automated systems contribute to unjustified different treatment or impacts disfavoring people based on their race, color, ethnicity, sex (including pregnancy, childbirth, and related medical conditions, gender identity, intersex status, and sexual orientation), religion, age, national origin, disability, veteran status, genetic information, or any other classification protected by law. Depending on the specific circumstances, such algorithmic discrimination may violate legal protections. Designers, developers, and deployers of automated systems should take proactive and continuous measures to protect individuals and communities from algorithmic discrimination and to use and design systems in an equitable way. This protection should include proactive equity assessments as part of the system design, use of representative data and protection against proxies for demographic features, ensuring accessibility for people with disabilities in design and development, pre-deployment and ongoing disparity testing and mitigation, and clear organizational oversight. Independent evaluation and plain language reporting in the form of an algorithmic impact assessment, including disparity testing results and mitigation information, should be performed and made public whenever possible to confirm these protections. *[Emphasis added]*

The common feature of the five highlighted bills and the Blueprint for an AI Bill of Rights excerpts is that they include general requirements for AI companies to disclose key elements of their systems, sometimes explicitly mentioning source code, as does the Justice in Forensic Algorithms Act of 2021, to federal authorities, independent auditors, or researchers. These requirements directly contradict the USMCA Article 19.16 obligation to not mandate the "*transfer of, or access to, a source code of software (…), or to an algorithm expressed in that source code, as a condition for the (…) distribution, sale or use of that software, or of products containing that software, in its territory.*" The Facial Recognition Act of 2022 and the Justice in Forensic Algorithms Act of 2021 clearly state that the regulated algorithmic software cannot be used in the United States unless these systems are tested by the Commerce Department's National Institute of Standards and Technology. And testing algorithms for biases, accuracy, and effectiveness generally requires source code disclosure,[23] which is precisely what a source code secrecy guarantee in a trade agreement would forbid.

It is worth noting that the specific exception to the secrecy guarantees included in USMCA Article 19.16.2 would not cover the sorts of policies proposed in these bills. The exception covers source code disclosure requests or orders by regulatory bodies or judicial authorities "*for a specific investigation, inspection, examination, enforcement action, or judicial proceeding*" (*emphasis added*). Insofar as most of these policies constitute general disclosure requirements, they are not protected by this exception. This is an especially pernicious feature of this limited exception in USMCA. Effectively, the exception covers the situation of a government agency or private party having sufficient evidence of the violation of a law or right to meet a burden of proof to be able to obtain more information, whether through an agency investigation, court order, or civil suit discovery. Yet it may well not be possible to meet that burden of proof without having access to the information about the source code or algorithm that reveals the civil rights or other violation.

In the case of the Platform Accountability and Transparency Act, indeed, the U.S. government could argue that platforms would only have to disclose information to authorized researchers for *specific* qualified research projects and, thus, claim that the exception is applicable. It is worth noting that the definition of "qualified data and information" included in Section 2 of this bill is broad and could encompass source code or other algorithm-related data, particularly considering that the aim of the legislation is to increase transparency over the impact that social media platforms have on our lives. This is the rationale behind requiring certain tech companies to disclose key information and data to qualified researchers for authorized academic projects. Unfortunately, it is unclear whether a research project, albeit authorized and buttressed by governmental authorities, would fall under the exception's notion of "*investigation, inspection, examination, enforcement action, or judicial proceeding*" of USMCA Article 19.16.2 given

23 Irion, Kristina (2021). "AI regulation in the European Union and Trade Law: How Can Accountability of AI and a High Level of Consumer Protection Prevail over a Trade Discipline on Source Code?" p. 25-26, Jan. 26, 2021. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3786567.

that these terms point toward administrative or judicial action, not academic projects. This potential incompatibility further shows how imposing limits via international rules, only changeable by consensus of numerous countries, on domestic policymaking with respect to an ever-changing, frontier sector of the economy is extremely risky.

Finally, the specific language of the provision forbidding governments to do exactly what the five example U.S. bills require is framed in the context of a government of one country requiring such access or review for the software owned by a person from another agreement-signatory country. This sort of framing is common in trade agreement texts. It appears to allow a government to do whatever it chooses to its domestic firms, while only limiting what policies can be applied to foreign firms, goods, or services. However, practically, such provisions set a standard that will become the domestic law and practice. First, politically, no government will provide foreign firms what domestic firms would see as privileged treatment in the home market. Second, practically, even if they did, a large multinational firm could demand any "more favorable treatment" given to foreign firms by simply setting up a foreign subsidiary in another agreement-signatory country and claiming that the rule is thus applicable to it. Trade law is rife with examples of corporations adopting "nationalities of convenience" and of industry allies operating across borders to use trade pacts to knock down policies they oppose. Some now in Congress may recall the National Cattlemen's Beef Association cheering on other countries' World Trade Organization (WTO) challenge against meat country of origin labeling rules, which the U.S. industry had been unable to kill in Congress, agencies, or courts.[24] Another related example is the infamous practice of "treaty-shopping," by which multinational firms engage in corporate planning to gain access to the most favorable Investor-State Dispute Settlement (ISDS) rules with the explicit purpose of establishing subsidiaries to lodge ISDS claims against countries they otherwise could not touch.

II. Guarantees of Tech Firms' Control of Data, Including Rights to Move, Process, and Store Personal Data Wherever the Firms Choose

Until recently, the corporations running digital platforms have had free rein to move data across borders without any restrictions, process it wherever they choose, and store the data wherever it is cheapest to do so. While the expansion of data flows can contribute to knowledge diffusion and international connectedness, there are many compelling reasons to regulate how certain kinds of data may be collected, where they can be processed or transmitted, and how, where, and for how long they are stored.

There is a growing consensus about the need to regulate the use and collection of personal data to protect consumers' privacy and the security of their personal data. The EU General Data Protection Regulation (GDPR) began to set a global standard. It

24 "Preliminary COOL ruling good for cattlemen," National Cattlemen's Beef Association, May 31, 2011. Available at: https://www.farmprogress.com/livestock/ncba-preliminary-cool-ruling-good-cattlemen; NCBA Comments on WTO Ruling on COOL, Jul. 2 2012. Available at: https://www.thebeefsite.com/news/39031/ncba-comments-on-wto-ruling-on-cool.

requires that companies collecting or processing EU residents' data comply with fairly strict transparency, accountability, and data minimization requirements. Under the GDPR, firms must process data for the legitimate purposes for which it is collected, refrain from collecting more data than necessary, keep information accurate and updated, and ensure that processing is done in a way that guarantees data security. To guarantee compliance with these obligations, the EU mandates that data can only be transferred to countries where adequate standards of protection are in place.[25] Alternatively, data can be transferred to third countries under binding corporate rules (BCRs) for intra-company transfers or standard contractual clauses (SCCs) for transfers between companies. In both of these circumstances, the entity located in an EU member state must accept liability for any breach of the GDPR by an entity not established in the EU.[26]

In cases where the European Commission has tried to bypass this key element of the GDPR, for instance by allowing data transfers to the United States despite the lack of national data privacy legislation here, the European Court of Justice has invalidated the Commission's adequacy determinations.[27]

In the United States, the American Data Privacy and Protection Act has been praised by privacy experts because it incorporates core tenets of a working data privacy and security regime. Among them, it includes a substantial set of individual rights, as well as strong data controller obligations. However, those rights and obligations could be weakened because the legislation neither limits transfers of data to offshore processors, over whom the U.S. government's enforcement powers could be limited, nor adds special liability for a covered entity that makes such transfers. Yet the various mechanisms that could ensure the proposal's effectiveness is not eroded by firms, as moving data offshore would likely collide with Big Tech demands for digital trade rules that guarantee unlimited rights to cross-border movement of data and to process and store personal data wherever the firms choose.

The chart below displays the USMCA articles that include the dual cross-border data flows and anti-data localization rules and the provisions of the ADPPA, along with other federal data privacy bills and their conflicts with the Big Tech "digital trade" agenda.

25 Article 45 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).

26 Article 47.2(f) of the GDPR and Clause 12(b) of the Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

27 European Court of Justice, Schrems v Data Protection Commissioner (2015), Case C-362/14; European Court of Justice, Schrems and Facebook Ireland v Data Protection Commissioner (2020), Case C-311/18.

USMCA Article 19.11: Cross-Border Transfer of Information by Electronic Means

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.[5]

USMCA Article 19.12: Location of Computing Facilities

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.

[5] 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.

Threatened Domestic Policy Initiatives	Provisions
American Data Privacy and Protection Act (H.R.8152) Sponsor: Rep. Frank Pallone Jr. (D-NJ). Cosponsors: Rep. Cathy McMorris Rodgers (R-WA), Rep. Janice Schakowsky (D-IL), and Rep. Gus Bilirakis (R-FL). *[Senate Commerce Committee Ranking Member Sen. Roger Wicker (R-MS) also backs the bill.]*	SEC. 203. INDIVIDUAL DATA OWNERSHIP AND CONTROL. ACCESS TO, AND CORRECTION, DELETION, AND PORTABILITY OF, COVERED DATA.—Subject to subsections (b) and (c), a covered entity shall provide an individual, after receiving a verified request from the individual, with the right to— (1) access— (A) the covered data (...) (B) the name of any third party and the categories of any service providers to whom the covered entity has transferred for consideration the covered data of the individual, as well as the categories of sources from which the covered data was collected; and (C) a description of the purpose for which the covered entity transferred the covered data of the individual to a third party or service provider; (2) correct any verifiably material inaccuracy or materially incomplete information with respect to the covered data of the individual that is processed by the covered entity and instruct the covered entity to notify any third party, or service provider to which the covered entity transferred such covered data of the corrected information; (3) delete covered data of the individual that is processed by the covered entity and instruct the covered entity to notify any third party, or service provider to which the covered entity transferred such covered data of the individual's deletion request; (...) SEC. 206. THIRD-PARTY COLLECTING ENTITIES. (...) (b) Third-Party Collecting Entity Registration.—

	(1) IN GENERAL.—Not later than January 31 of each calendar year that follows a calendar year during which a covered entity acted as a third-party collecting entity and processed covered data pertaining to more than 5,000 individuals or devices that identify or are linked or reasonably linkable to an individual, such covered entity shall register with the Commission in accordance with this subsection. (...) (3) THIRD-PARTY COLLECTING ENTITY REGISTRY.—The Commission shall establish and maintain on a website a searchable, publicly available, central registry of third-party collecting entities that are registered with the Commission under this subsection that includes the following: (A) A listing of all registered third-party collecting entities and a search feature that allows members of the public to identify individual third-party collecting entities. (B) For each registered third-party collecting entity, the information described in paragraph (2). (C) A "Do Not Collect" registry link and mechanism by which an individual may, after the Commission has verified the identity of the individual or individual's parent or guardian, which may include tokenization, easily submit a request to all registered third-party collecting entities that are not consumer reporting agencies, and to the extent they are not acting as consumer reporting agencies, as defined in section 603(f) of the Fair Credit Reporting Act () to— (i) delete all covered data related to such individual that the third-party collecting entity did not collect from the individual directly or when acting as a service provider; and (ii) ensure that any third-party collecting entity no longer collects covered data related to such individual without the affirmative express consent of such individual, except insofar as such covered entity is acting as a service provider. Each third-party collecting entity that receives such a request from an individual shall delete all the covered data of the individual not later than 30 days after the request is received by the third-party collecting entity. *[Emphasis added]*
My Body, My Data Act of 2022 (H.R.8111/S.4434) Sponsors: Rep. Sara Jacobs (D-CA) and Sen. Mazie Hirono (D-HI).	SEC. 2. MINIMIZATION. (a) Minimization Of Collecting, Retaining, Using, And Disclosing.—A regulated entity may not collect, retain, use, or disclose personal reproductive or sexual health information except— (1) with the express consent of the individual to whom such information relates; or (2) as is strictly necessary to provide a product or service that the individual to whom such information relates has requested from such regulated entity. (...)

Cosponsors: 116 representatives and 12 senators.[28]	(b) Right Of Deletion.—A regulated entity shall make available a reasonable mechanism by which an individual, upon a verified request, may request the deletion of any personal reproductive or sexual health information relating to such individual that is retained by such regulated entity, including any such information that such regulated entity collected from a third party or inferred from other information retained by such regulated entity.

28 Full list of cosponsors (accessed Nov. 15, 2022): Rep. Ann Kuster (D-NH), Rep. Dean Phillips (D-MN), Rep. Lois Frankel (D-FL), Rep. Ayanna Pressley (D-MA), Rep. Judy Chu (D-CA), Rep. Sylvia Garcia (D-TX), Rep. Anna Eshoo (D-CA), Rep. Jackie Speier (D-CA), Rep. Julia Brownley (D-CA), Rep. Kathy Manning (D-NC), Rep. Brenda Lawrence (D-MI), Rep. Shelia Jackson Lee (D-TX), Rep. Donald Payne (D-NJ), Del. Eleanor Holmes Norton (D-DC), Rep. Juan Vargas (D-CA), Rep. Earl Blumenauer (D-OR), Rep. Jake Auchincloss (D-MA), Rep. Susan Wild (D-PA), Rep. Jason Crow (D-CO), Rep. Melanie Ann Stansbury (D-NM), Rep. Nikema Williams (D-GA), Rep. Veronica Escobar (D-TX), Rep. Jahana Hayes (D-CT), Rep. Carolyn Maloney (D-NY), Rep. Robin L. Kelly (D-IL), Rep. Susie Lee (D-NV), Rep. Grace Meng (D-NY), Rep. Katherine M. Clark (D-MA), Rep. Deborah Ross (D-NC), Rep. Ro Khanna (D-CA), Rep. Mary Gay Scanlon (D-PA), Rep. Marie Newman (D-IL), Rep. Alan S. Lowenthal (D-CA), Rep. Barbara Lee (D-CA), Rep. Teresa Leger Fernandez (D-NM), Rep. Lizzie Fletcher (D-TX), Rep. Ritchie Torres (D-NY), Rep. Zoe Lofgren (D-CA), Rep. Norma J. Torres (D-CA), Rep. Steve Cohen (D-TN), Rep. Lucile Roybal-Allard (D-CA), Rep. Raja Krishnamoorthi (D-IL), Rep. Suzanne Bonamici (D-OR), Rep. Gwen Moore (D-WI), Rep. Betty McCollum (D-MN), Rep. Jamaal Bowman (D-NY), Rep. Tim Ryan (D-OH), Rep. Mark DeSaulnier (D-CA), Rep. Albio Sires (D-NJ), Rep. Ami Bera (D-CA), Rep. Katie Porter (D-CA), Rep. Lloyd Doggett (D-TX), Rep. Mike Quigley (D-IL), Rep. James McGovern (D-MA), Rep. Nanette Diaz Barragan (D-CA), Rep. Frederica S. Wilson (D-FL), Rep. Bonnie Watson Coleman (D-NJ), Rep. Colin Allred (D-TX), Rep. Dina Titus (D-NV), Rep. Diana DeGette (D-CO), Rep. Jared Huffman (D-CA), Rep. Joseph Morelle (D-NY), Rep. Eddie Bernice Johnson (D-TX), Rep. Abigail Davis Spanberger (D-VA), Rep. Chris Pappas (D-NH), Rep. Daniel Kildee (D-MI), Rep. Adam Schiff (D-CA), Rep. Steven Horsford (D-NV), Rep. Val Butler Demings (D-FL), Rep. Paul Tonko (D-NY), Rep. Sean Casten (D-IL), Rep. Lisa Blunt Rochester (D-DE), Rep. Tom O'Halleran (D-AZ), Rep. Mark Takano (D-CA), Rep. Donald Beyer, Jr. (D-VA), Rep. Shelia Cherfilus-McCormick (D-FL), Rep. Tony Cárdenas (D-CA), Rep. David Trone (D-MD), Rep. Mondaire Jones (D-NY), Rep. Donald McEachin, (D-VA), Rep. Ruben Gallego (D-AZ), Rep. Rashida Tlaib (D-MI), Rep. Anthony Brown (D-MD), Rep. Brad Sherman (D-CA), Rep. Raul Ruiz (D-CA), Rep. John Yarmuth (D-KY), Rep. Josh Gottheimer (D-NJ), Rep. Chellie Pingree (D-ME), Rep. Ed Perlmutter (D-CO), Rep. Joaquin Castro (D-TX), Rep. Tom Malinowski (D-NJ), Rep. Joe Neguse (D-CO), Rep. Debbie Wasserman Schultz (D-FL), Rep. Pramila Jayapal (D-WA), Rep. Gregory Meeks (D-NY), Rep. Andre Carson (D-IN), Rep. Eric Swalwell (D-CA), Rep. Ann Kirkpatrick (D-AZ), Rep. Adam Smith (D-WA), Rep. Grace Napolitano (D-CA), Rep. Marc A. Veasey (D-TX), Rep. Hakeem Jeffries (D-NY), Rep. Al Lawson, Jr. (D-FL), Rep. Mark Pocan (D-WI), Rep. Jamie Raskin (D-MD), Rep. Salud Carbajal (D-CA), Rep. Jennifer Wexton (D-VA), Rep. Lori Trahan (D-MA), Rep. Mikie Sherrill (D-NJ), Rep. William Keating (D-MA), Rep. Greg Stanton (D-AZ), Rep. Elaine Luria (D-VA), Rep. Kim Schrier (D-WA), Rep. Pete Aguilar (D-CA), Rep. Mike Levin (D-CA), Rep. Doris Matsui (D-CA), Sen. Ron Wyden (D-OR), Sen. Kirsten Gillibrand (D-NY), Sen. Tina Smith (D-MN), Sen. Sheldon Whitehouse (D-RI), Sen. Richard Blumenthal (D-CT), Sen. Tammy Baldwin (D-WI), Sen. Sherrod Brown (D-OH), Sen. Tammy Duckworth (D-IL), Sen. Amy Klobuchar (D-MN), Sen. Cory Booker (D-NJ), Sen. Maria Cantwell (D-WA), and Sen. Jeanne Shaheen (D-NH).

Fourth Amendment Is Not For Sale Act (S.1265/H.R.2738) Sponsors: Sen. Ron Wyden (D-OR) and Rep. Jerrold Nadler (D-NY). Cosponsors: 22 senators.[29]	**SEC. 4. INTERMEDIARY SERVICE PROVIDERS.** (a) Definition.—Section 2711 of title 18, United States Code, is amended— (...) (3) by adding at the end the following: "(5) the term 'intermediary service provider' means an entity or facilities owner or operator that directly or indirectly delivers, stores, or processes communications for or on behalf of a provider of electronic communication service to the public or a provider of remote computing service." (b) Prohibition.—Section 2702(a) of title 18, United States Code, is amended— (...) (4) by adding at the end the following: "(4) an intermediary service provider shall not knowingly divulge— "(A) to any person or entity the contents of a communication while in electronic storage by that provider; or "(B) to any governmental entity a record or other information pertaining to a subscriber to or customer of, a recipient of a communication from a subscriber to or customer of, or the sender of a communication to a subscriber to or customer of, the provider of electronic communication service to the public or the provider of remote computing service for, or on behalf of, which the intermediary service provider directly or indirectly delivers, transmits, stores, or processes communications."
Protecting Americans' Data From Foreign Surveillance Act of 2022 (S.4495) Sponsor: Sen. Ron Wyden (D-OR). Cosponsors: Sen. Cynthia Lummis (R-WY), Sen. Sheldon Whitehouse (D-RI), Sen. Marco Rubio (R-FL), and Sen. Bill Hagerty (R-TN).	**SEC. 3. REQUIREMENT TO CONTROL THE EXPORT OF CERTAIN PERSONAL DATA OF UNITED STATES NATIONALS AND INDIVIDUALS IN THE UNITED STATES.** (a) In General.—Part I of the Export Control Reform Act of 2018 (50 U.S.C. 4811 et seq.) is amended by inserting after section 1758 the following: "SEC. 1758A. REQUIREMENT TO CONTROL THE EXPORT OF CERTAIN PERSONAL DATA OF UNITED STATES NATIONALS AND INDIVIDUALS IN THE UNITED STATES. (...) "(b) Commerce Controls.— "(1) CONTROLS REQUIRED.—Beginning 18 months after the date of the enactment of the Protecting Americans' Data From Foreign Surveillance Act of 2022, the Secretary shall impose appropriate controls under the Export Administration Regulations on the export or reexport to, or in-country transfer in, all countries (other than countries on the list required by paragraph (2)(D)) of covered personal data in a manner that exceeds the applicable threshold established under subsection (a)(3), including through

29 Full list of cosponsors (accessed Nov. 15, 2022): Sen. Rand Paul (R-KY), Sen. Patrick Leahy (D-VT), Sen. Mike Lee (R-UT), Sen. Edward Markey (D-MA), Sen. Steve Daines (R-MT), Sen. Tammy Baldwin (D-WI), Sen. Elizabeth Warren (D-MA), Sen. Sherrod Brown (D-OH), Sen. Brian Schatz (D-HI), Sen. Cory Booker (D-NJ), Sen. Bernard Sanders (I-VT), Sen. Jeff Merkley (D-OR), Sen. Jon Tester (D-MT), Sen. Martin Heinrich (D-NM), Sen. Mazie Hirono (D-HI), Sen. Patty Murray (D-WA), Sen. Charles Schumer (D-NY), Sen. Richard Blumenthal (D-CT), Sen. Maria Cantwell (D-WA), Sen. Tammy Duckworth (D-IL), Sen. Ben Ray Lujan (D-NM), and Rep. Zoe Lofgren (D-CA).

	interim controls (such as by informing a person that a license is required for export, reexport, or in-country transfer of covered personal data), as appropriate, or by publishing additional regulations. "(2) LEVELS OF CONTROL.— "(A) IN GENERAL.—Except as provided in subparagraph (C) or (D), the Secretary shall— "(i) require a license or other authorization for the export, reexport, or in-country transfer of covered personal data in a manner that exceeds the applicable threshold established under subsection (a)(3); "(ii) determine whether that export, reexport, or in-country transfer is likely to harm the national security of the United States—" "(I) after consideration of the matters described in subparagraph (B); and "(II) in coordination with the heads of the appropriate Federal agencies; and "(iii) if the Secretary determines under clause (ii) that the export, reexport, or in-country transfer is likely to harm the national security of the United States, deny the application for the license or other authorization for the export, reexport, or in-country transfer.

In the absence of U.S. national policies regarding what data may be collected from users and where and how it can be processed and stored, private firms prioritizing their business goals have been able to exploit people's data for commercial surveillance and sell personal information to law enforcement agencies, among other abuses. How to effectively protect peoples' privacy, or even enforce existing privacy protections that current law confers for certain sensitive data, such as health data under the Health Insurance Portability and Accountability Act or financial data under statutes such as the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act as amended by the Fair and Accurate Credit Transactions Act, has proven to be a daunting endeavor. As legislators are working to address these challenges and narrower data-related threats, such as the use of geolocation data to track women who may seek abortions or companies targeting children and teenagers to advertise unsafe products, tech interests who profit from buying, selling, and otherwise exploiting our private data are seeking terms in trade pacts and policies that make limits on data flows "illegal trade barriers."

Three examples of the conflict and threats are demonstrated by ADPPA, the My Body, My Data Act of 2022, and the Fourth Amendment Is Not For Sale Act. Each of these bills seeks to provide users with protections related to their data. But all of them have loopholes due to the difficulties of enforcing these U.S. legal protections with respect to data that has been moved outside the United States.

One approach is provided by ADPPA, the main obligations of which are imposed on "covered entities" and, in some cases, "service providers." These are firms that process, store, or transfer data on behalf of a covered entity. A covered entity is, broadly, an entity that determines the purposes and means of collecting, processing, or transferring covered

data and is either subject to the Federal Trade Commission Act or the Communications Act of 1934 (see Sec. 2(9)). ADPPA also imposes some obligations on third parties, which are companies that collect and process data but are not service providers for covered entities.

While imposing some limitations, this legislation does not forbid transferring data to service providers or third parties located abroad. The offshoring of personal data is allowed as long as it complies with ADPPA's general data minimization rule, which is that the operation is deemed necessary and proportionate and it is carried out under one of the permissible purposes listed in the bill (see Sec. 101). Covered parties could even transfer sensitive personal data to third parties, even if located abroad, if they get the consent from the relevant individual (see Sec. 102(a)(3)(A)).

Under ADPPA, when transferring data to service providers, covered entities must enter in a contract with service providers that, among other elements, does not relieve them from the obligations established by the law. However, covered entities as a general rule are not liable for any breach of the law carried out by a service provider (see Section 302(c)(2)), unlike the system put in place in the EU by the GDPR. Moreover, there are no statutory requirements for contracts between covered entities and third parties in the bill.

Then, when an individual attempts to exercise their rights to correct information or demand deletion of data as provided by this legislation, a covered entity has an obligation to do so. Plus, ADPPA compels the covered entity to notify any relevant service provider or third party that an individual has made such requests (see Sec. 203(a)(2) and (3)). However, if a service provider or a third party chooses not to abide by these requests, the individual would not have effective recourse to demand compliance, the U.S. government would have limited ways to enforce the law, and neither the covered entity nor the third party or service provider would face any sanction.

Additionally, while the ADPPA requires registration of third-party collecting entities and the establishment by the Federal Trade Commission of a central registry of these entities that includes a "Do Not Collect" mechanism by which individuals could demand deletion of their personal information and guarantees that any third-party collecting entity will not collect their data without their consent, it is unclear how this protection is enforceable against third-party entities located abroad.

Fixing these loopholes would improve the efficacy of the bill. The GDPR adequacy system, albeit imperfect, creates some safeguards for individuals seeking to protect their privacy and data security.

Yet adding a similar system – or a stronger one – would conflict with the digital trade agreement terms that the industry seeks, which would guarantee unfettered cross-border data flows and ban limits on where data may be processed or stored.

Similarly, if the My Body, My Data Act of 2022 rights are to be effective, legislators must include means to control offshoring of personal reproductive data. This legislation came

in the aftermath of the Supreme Court's *Dobbs v. Jackson* ruling and discussion in some states about criminal prosecution against women seeking abortions or those willing to aid their access to such health care. This in turn raised the specter of police seeking to get data from period and pregnancy tracker apps and/or geolocation data to investigate and prosecute women and those who assist them. An investigation by Forbes showed that two of the most popular pregnancy and ovulation trackers, with downloads in excess of 15 million on Google's Android app store alone, have lax privacy policies and reserve the right to share data with law enforcement at their discretion. Moreover, these apps share collected data with several third parties, including Facebook and various ad trackers, such as Taboola, ScorecardResearch, Magnite, Adjust, and Upland Software, increasing the ways in which law enforcement agencies can get their hands on personal reproductive data.[30] Some of these companies are not headquartered in the United States. For instance, Adjust is based in Berlin,[31] and while a company located in Germany would have to comply with the GDPR, a firm could easily establish itself or create a subsidiary in a jurisdiction without any kind of data privacy regulation and where the safeguards of the My Body, My Data Act of 2022 would not apply.

Arguably, the most important provision of the My Body, My Data Act of 2022 is the right to deletion, which establishes that a "*regulated entity shall make available a reasonable mechanism by which an individual, upon a verified request, may request the deletion of any personal reproductive or sexual health information relating to such individual that is retained by such regulated entity, including any such information that such regulated entity collected from a third party or inferred from other information retained by such regulated entity.*"

Yet the regulated entity does not have an obligation to ensure that the data subject to a deletion request is effectively deleted by the third parties to whom it might have transferred the data. The My Body, My Data Act does not even have the lesser obligation of notifying third parties of the deletion request, which ADPPA does have. Thus, any third party that is not subject to this legislation's requirements could keep storing the sensitive data, particularly entities that are located abroad, and sell it to law enforcement agencies interested in using the information for criminal investigations.

This is not a hypothetical risk. In August 2022, the Federal Trade Commission filed a lawsuit against data broker Kochava Inc. for selling geolocation data from hundreds of millions of mobile devices that can be used to trace the movements of individuals to and from sensitive locations. Kochava sells, among other types of data, information that can reveal people's visits to reproductive health clinics.[32] Law enforcement agencies are some

30 Thomas Brewster, "15 Million Downloaded Pregnancy Trackers That May Give Data To Cops Without A Warrant – Should You Worry?" Forbes, Jun. 29, 2022. Available at: https://www.forbes.com/sites/thomasbrewster/2022/06/29/ziff-davis-pregnancy-trackers-may-give-data-to-cops-without-a-warrant/?utm_campaign=socialflowForbesMainTwitter&utm_medium=social&utm_source=-ForbesMainTwitter&sh=21a16ac5710c.

31 Adjust, "Our offices." Available at: https://www.adjust.com/company/offices/.

32 "FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations," Federal Trade Commission, Aug. 29, 2022. Available at: https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

of the main clients for these kinds of data. In September 2022, an Associated Press report unveiled how nearly two dozen agencies in about 40 contracts purchased a software that allows local police departments to search hundreds of billions of records from 250 million mobile devices and harness the data to be used in criminal investigations.[33]

This practice is precisely the focus of the Fourth Amendment Is Not For Sale Act. If passed, the bill would prevent law enforcement and intelligence agencies from buying people's personal data from data brokers for criminal prosecution purposes. Equally important, the bill bans these data brokers, officially named intermediary service providers, from divulging personal communications and records in general and without a court order to government agencies. Again, the issue with this important bill is that obligations to intermediary service providers are only enforceable for those companies located in U.S. jurisdiction.

To truly neutralize the risk of personal reproductive data being used against women and those aiding women seeking to exercise their reproductive health rights, the My Body, My Data Act should include strong protections against data offshoring. Similarly, the Fourth Amendment Is Not For Sale Act should factor in the risks of data brokers having data hubs offshore. Yet the fixes needed to these proposals to ensure that they meet their privacy goals conflict with the data free-flow rules in USMCA.

The fact that USMCA Article 19.12 includes an outright ban on data localization requirements, without exception, shows why this cannot be the model for digital rules going forward. Such an approach would pose a major hurdle for legislators who conclude that certain sensitive personal data, perhaps including reproductive information, must be held in the United States to ensure that U.S. law covers the relevant entities dealing with the data and that such entities are subject to enforcement action so as to ensure the privacy of the covered personal data.

Alternatively, if policymakers would attempt to regulate cross-border data flows by including an adequacy system or similar mechanism, that would likely constitute a "restriction on the cross-border transfer of information," again showing why the USMCA standard is a non-starter.

An example of a policy that directly and clearly conflicts with USMCA's unfettered movement of data guarantees is the Protecting Americans' Data From Foreign Surveillance Act of 2022. This bipartisan bill would enact export controls stopping or limiting the transfer offshore of certain personal data of American citizens when such a transfer would threaten U.S. national security. The bill's default rule is that the movement of certain data offshore, if above certain thresholds, would be subject to controls. Only a set of countries to be included in a positive list, as defined by regulators, would be eligible to receive personal data from Americans without being subject to controls. The inconsistency with USMCA's free cross-border transfer of data obligation of a proposal

33 Garence Burke and Jason Dearen, "Tech tool offers police 'mass surveillance on a budget,'" AP News, Sept. 2 2022. Available at: https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef.

of this nature, which includes bans on some data flows and limits on data flows via licensing, is evident.

Notably, that USMCA term has an exception in its second paragraph. However, the exception replicates controversial terms of the General Agreement on Trade and Tariffs general exceptions, which made these affirmative defenses virtually ineffective. Namely, USMCA Article 19.11.2 allows policies that are "necessary" to achieve a legitimate public policy objective, provided that the policy: (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.

But countries have rarely been able to meet these showings. Two-thirds of countries' attempts to prove that a public interest policy is "necessary" under the WTO Dispute Settlement system have failed.[34] This is due to an important degree to the requirement in condition (b) of USMCA Article 19.11.2: Namely, a policy must "*not impose restrictions on transfers of information greater than are necessary to achieve the objective*." This means that if a U.S. policy that regulates cross-border data flows to safeguard reproductive rights, for instance, is challenged under trade-pact language that is based on the expansive rights for company control of data established in USMCA, a trade tribunal might decide that there are other ways in which the United States could have an *equivalent contribution* to this objective that are *less trade restrictive* and, thus, rule that the policy is an illegal trade barrier that must be eliminated.

Equally controversial is condition (a) of the exception, which requires that the policy "*is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade*." Of the 48 cases where WTO countries have tried to use the general exception defenses, in only 14 has a WTO tribunal even proceeded to this test. In WTO law, this is the last step of the analysis to justify a policy under the general exceptions and most cases are thrown out on the "necessary" test or other earlier hurdles. Of the 14 cases that faced this test, 12 failed. Indeed, the WTO defense that is parallel to this USMCA exception has only been allowed in two of 48 attempts.[35] Legal scholars like Duke University Law School Professor Tim Meyer have concluded that this high failure rate is explained by the lack of consideration that the "*arbitrary or unjustifiable discrimination or a disguised restriction on trade*" language gives to the nature of domestic policymaking.[36] Thus, the ostensible "exception" provided by USMCA Article 19.2 in fact provides no safeguard for policymakers aiming to regulate the movement of data, whether this is done to protect personal data privacy and security or for national security purposes, among other important societal public policy objectives.

34 Daniel Rangel, "WTO General Exceptions: Trade Law's Faulty Ivory Tower," Public Citizen's Global Trade Watch, Jan. 2022. p. 18-19. Available at: https://www.citizen.org/article/wto-general-exceptions-trade-laws-faulty-ivory-tower/.

35 Ibid. p. 21.

36 Timothy Meyer, "The Political Economy of WTO Exceptions," Washington University Law Review, Vol. 99, Apr. 1, 2021. Vanderbilt Law Research Paper No. 21-18, Available at SSRN: https://ssrn.com/abstract=3817719 or http://dx.doi.org/10.2139/ssrn.3817719.

III. Designation of Key Anti-Monopoly Policies as Discriminatory Illegal Trade Barriers Via Open-Ended "Non-Discrimination" Standards

Numerous countries are starting to take action against Big Tech monopoly abuses. Within six months of being sworn in, President Biden declared anti-monopoly work a whole-of-government priority, issuing an Executive Order on Promoting Competition in the American Economy.[37] During the last decades, predatory behavior and lax antitrust enforcement,[38] along with network effects and "winner-take-all" dynamics in digital markets,[39] have led to monopolies in the digital services that the vast majority of people use daily. After years of abuses, and advocacy from smaller businesses, consumers, and workers in response, policymakers worldwide have begun introducing policies to rein in the largest few Big Tech entities, which have extreme dominance over the digital economy. Some of the most common measures aim at increasing competition by setting rules on app store operators; forbidding certain anticompetitive practices from digital "gatekeepers"; addressing the power imbalance between media outlets and the mega-platforms that currently determine what kind of content ends up reaching the public; and stopping anticompetitive behavior before it happens.

Big Tech is spending billions fighting these efforts. One powerful under-the-radar strategy has been to hijack the international trade law concept of "non-discrimination" to use trade enforcement mechanisms to attack other countries' policies that constrain digital platforms' monopolistic size and anticompetitive behavior. Big Tech interests are seeking to harness U.S. domestic trade enforcement tools, such as the annual National Trade Estimate (NTE) reporting system, to try to roll back or chill establishment of strong policies in other countries. Getting such policies in other nations labeled as illegal trade barriers would also undermine the domestic push for greater regulation in the United States. And, when deployed in the context of ongoing trade negotiations, this strategy is also aimed at preventing regulation in the United States by locking in binding constraints on domestic policy within international trade pact rules to set a global standard against anti-monopoly policies and tools being deployed here and abroad.

The non-discrimination concept is as old as the first trade agreements. In its most basic form, it requires countries to treat products the same regardless of national origin. When applied to trade in goods, that means a country must provide an imported good with the same treatment it gives to its own producers' "like" goods and also not treat the imported goods from one country differently than those from another country. For instance, if a

37 Executive Order 14036, "Promoting Competition in the American Economy," Jul. 9, 2021. Available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/.

38 Matt Stoller, Sarah Miller, and Zephyr Teachout, "Addressing Facebook and Google's Harms Through a Regulated Competition Approach," American Economic Liberties Project, Apr. 10, 2020. Available at: https://www.economicliberties.us/our-work/addressing-facebook-and-googles-harms-through-a-regulated-competition-approach/; Matt Stoller, Pat Garofalo, and Olivia Webb, "Understanding Amazon: Making the 21st-Century Gatekeeper Safe for Democracy," American Economic Liberties Project, Jul. 24, 2020. Available at: https://www.economicliberties.us/our-work/understanding-amazon-making-the-21st-century-gatekeeper-safe-for-democracy/.

39 Mariana Mazzucato, "Preventing Digital Feudalism," Project Syndicate, Oct. 2, 2019. Available at: https://www.project-syndicate.org/commentary/platform-economy-digital-feudalism-by-mariana-mazzucato-2019-10; the House Antitrust Report on Big Tech, Oct. 6, 2020. Available at: https://www.nytimes.com/interactive/2020/10/06/technology/house-antitrust-report-big-tech.html.

country allowed the use of a pesticide domestically, it could not ban imported food grown elsewhere using the same chemical, or that imports from one country with a particular pesticide residue are allowed in but are banned from a different country. Thus, initially, the non-discrimination standard especially targeted facially discriminatory policies or those that had a clearly discriminatory intent. However, as trade pacts expanded into setting rules applicable to the service sector and other areas of regulation that previously had been the sole bailiwick of domestic policymaking, commercial interests eager to overcome local standards to maximize access to other nations' markets pushed to expand the standard. Most trade pacts signed since the 1990s include language that can be used to attack origin-neutral policies that may have a disproportionate effect on foreign products. And even before the language was broadened, trade-pact enforcement tribunals contributed to the perilous expansion of the non-discrimination standard by starting to rule that facially neutral policies with inadvertent differential impacts were illegal trade barriers.[40]

Big Tech is trying to take advantage of those expansive rules and interpretations to establish new grounds to attack policies around the world that attempt to regulate the most dominant digital corporations. **USMCA's digital trade "non-discrimination" provision is an example of the type of legal text that forbids domestic digital policies that may have a disproportionate effect.** Namely, that provision captures neutral policies that may have a larger impact on the largest firms simply because they are large. That is to say, even when the predominant underlying motive of a policy is not related to the place from which digital services are provided or the country of incorporation of said firms, a neutral domestic policy may have greater effect on firms that dominate a market. For example, consider a domestic policy that requires all domestic and foreign online ride-hailing services to register as taxi companies and meet policies applicable to other such firms. This neutral policy would not be considered discriminatory on its face, but it would have a greater effect on, say, Uber, if Uber had the largest share of a country's online ride-hailing services. The Coalition for App Fairness recently wrote to the Office of the United States Trade Representative (USTR) and Commerce Secretary urging that the IPEF not include the USMCA-TPP approach, which the business association notes would threaten the Biden administration's initiatives on competition.[41]

The chart below includes the relevant USMCA provision. Interestingly, earlier U.S. trade pacts with e-commerce rules included non-discrimination language that was explicitly devised to require proof of discriminatory intent in order to find a facially neutral policy that may have a differential impact on digital products from an agreement-signatory country compared to domestic products to be an illegal trade barrier. We provide a sample of this

40 For instance, in 1992, a panel under the General Agreement on Tariffs and Trade (GATT) determined that certain tax benefits provided to microbreweries in the United States were inconsistent with GATT Article III (national treatment) because larger Canadian beer producers could not access them. U.S. large breweries were also ineligible. See: Panel Report, United States – Measures Affecting Alcoholic and Malt Beverages, DS23/R, adopted 19 June 1992, BISD 39S/206. Available at: ttps://worldtradelaw.net/document.php?id=reports/gattpanels/usmaltbeverages.pdf.

41 Coalition for App Fairness letter to Ambassador Katherine Tai and Secretary Gina Raimondo, Jan. 11, 2023. Available at: https://subscriber.politicopro.com/f/?id=00000185-a32b-de44-a7bf-eb3fd9770000.

language, from the U.S.-Korea FTA (KORUS), in comparison to demonstrate why the USMCA language, which is also found in the TPP, cannot be the model for future pacts.

KORUS	USMCA
Article 15.3: Digital Products	Article 19.4: Non-Discriminatory Treatment of Digital Products
2. **Neither Party may accord less favorable treatment to some digital products than it accords to other like digital products** (a) on the basis that: ***[Note: This means that subparagraphs (i) and (ii) refer to de jure discrimination claims.]*** (i) the digital products receiving less favorable treatment are created, produced, published, stored, transmitted, contracted for, commissioned, or first made available on commercial terms in the territory of the other Party, or (ii) the author, performer, producer, developer, distributor, or owner of such digital products is a person of the other Party; or (b) **so as otherwise to afford protection to other like digital products that are created, produced, published, stored, transmitted, contracted for, commissioned, or first made available on commercial terms in its territory.** ***[Note: The "so as otherwise to afford protection" language means that for claims of de facto discrimination, discriminatory intent must be proven.]*** 3. Neither Party may accord less favorable treatment to digital products: (a) created, produced, published, contracted for, commissioned, or first made available on commercial terms in the territory of the other Party than it accords to like digital products created, produced, published, contracted for, commissioned, or first made available on commercial terms in the territory of a non-Party; or (b) whose author, performer, producer, developer, distributor, or owner is a person of the other Party than it accords to like digital products whose author, performer, producer, developer, distributor, or owner is a person of a non-Party. *[Emphasis added.]*	1. No Party shall accord **less favorable treatment** to a digital product created, produced, published, contracted for, commissioned, or first made available on commercial terms in the territory of another Party, or to a digital product of which the author, performer, producer, developer, or owner is a person of another Party, than it accords to other like digital products.[3] [3] For greater certainty, to the extent that a digital product of a non-Party is a "like digital product," it will qualify as an "other like digital product" for the purposes of Article 19.4.1 (Non-Discriminatory Treatment of Digital Products). *[**Note: This broad standard treats de facto and de jure discrimination claims the same:** If a policy has greater impact on some firms/digital services than others, it is considered discriminatory even if the reason is size of firm and is unrelated to nationality.]*

Recently, Rethink Trade published a report that analyzed dozens of submissions to the U.S. government and reveals a pattern of Big Tech interests trying to use trade "non-discrimination" lingo to undermine countries' anti-monopoly initiatives.[42] Rethink Trade reviewed NTE submissions, which provide industry an opportunity to list policies it wants the U.S. government to pursue as illegal trade barriers. For years, the NTE report issued by USTR has been used to attack as trade barriers other countries' public interest policies that various industries dislike. Now, Big Tech is seizing the process with attacks especially aimed at cutting-edge anti-monopoly policies promoting fair competition that countries around the world, including the United States, are considering. Among the foreign policies targeted in the NTE process are those also pending adoption by the U.S. Congress to end app store operators' duopoly abuses and address the power imbalance between media outlets and the mega-platforms that currently determine what kind of content ends up reaching the public. The targeted policies include:

- **South Korea's App Stores Law, which,** like ***S. 2730/H.R.5017 The Open App Markets Act***, requires app stores to allow diverse payment systems (not only their own) and to allow app developers to sell on other platforms;
- **Australia's News Media Bargaining Code**, a law similar to ***S.673/H.R.1735 The Journalism Competition and Preservation Act***, which remedies Big Tech platforms' monopolization of ad revenue and decimation of local journalism by creating the conditions for digital platforms to pay for the news they distribute;
- **EU's Digital Markets Act,** the European Union's crackdown against abusive behavior by dominant digital firms, which shares many elements of ***S.2992/H.R.3816 The American Innovation and Choice Online Act*** and the imposition of data portability and interoperability requirements on large online platforms of the ***H.R.3849 Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2021***;
- **EU's Digital Services Act**, which establishes consumer rights online like ***S.1896/ H.R.3611 The Algorithmic Justice and Online Platform Transparency Act***; and
- **Germany's GWB Digitization Act**, a competition law revamp that proactively prevents anticompetitive actions by the biggest digital players, which shares some elements with the ***S.3847/H.R.7101 Prohibiting Anticompetitive Mergers Act,*** such as restricting the anticompetitive behavior of dominant firms and modernizing antitrust law to deal with the realities of digital markets.

Rethink Trade's report documents 30 instances of industry associations' attacks in 2020 and 2021 against the five cutting-edge competition policies mentioned above using the NTE reporting process and the claim that the policies are discriminatory trade barriers. Rethink Trade's initial review of industry submissions filed last year for the

42 "'Digital Trade' Doublespeak: Big Tech's Hijack of Trade Lingo to Attack Anti-Monopoly and Competition Policies," Rethink Trade, Nov. 2, 2022. Available at: https://rethinktrade.org/fact-sheet/digital-trade-doublespeak-big-techs-hijack-of-trade-lingo-to-attack-anti-monopoly-and-competition-policies/.

2023 NTE report shows that Big Tech firms will try to use trade law and enforcement tools to target any country that dares to act against their abuses. The submissions of several industry associations that represent companies like Google and Facebook for the 2023 NTE reporting process zeroed in on Canada's proposed Online News Act. It is similar to the Australian News Media Bargaining Code and the U.S. Journalism Competition and Protection Act, which require dominant Big Tech platforms to share ad revenue with the outlets that actually produce the content the platforms monetize. For instance, the Computer & Communications Industry Association (CCIA) claimed that Canada's Online News Act:

> "would force 'digital news intermediaries'—targeted at two U.S. companies based on testimony from Parliament and analyses from the Parliamentary Budget Officer—to pay Canadian news publishers for any content of theirs reproduced in any way. (...) **The legislation is in conflict with several of Canada's international trade obligations**. These obligations include the U.S.-Mexico-Canada Free Trade Agreement Articles 14.4 (Investment) and 15.3 (Cross-border Services) regarding National Treatment; USMCA Articles 14.5 (Investment) and 15.4 (Cross-border Services) regarding Most-Favored Nation Treatment; USMCA Article 14.10 regarding Performance Requirements; **USMCA Article 19.4 regarding Non-Discriminatory Treatment of Digital Products**; and intellectual property obligations through the World Trade Organization's absorption of the Berne Convention and the right to quotation in the Agreement on Trade-Related Aspects of Intellectual Property Rights." (*Emphasis added.*)[43]

CCIA's submission is instructive about the importance of not repeating the USMCA digital trade "non-discrimination" article in IPEF, APEP, or TTC, given U.S. officials have said that these pacts will not include the investment or service sector chapter also cited by CCIA. That means that excluding the broad non-discrimination language from any "digital trade" chapter arising from these negotiations is essential to avoid providing new grounds for Big Tech firms to assault digital governance policies. In contrast, extending this kind of language in "digital trade" deals covering the countries that make up a substantial portion of the world economy would allow these firms to use these provisions to attack anti-monopoly policies affecting large, dominant digital firms.

Obviously, given many of the most problematic Big Tech monopoly firms are U.S.-based, this particular provision does not pose the greatest direct threat against U.S. policymaking relative to the damage to policymaking elsewhere, given certain U.S. digital firms' monopolistic position in the world's digital markets. However, the threat goes beyond derailing anti-monopoly initiatives in other countries. By undermining policies abroad that resemble the same anti-monopoly initiatives being promoted here, particularly when U.S. officials are successfully recruited to join the attacks, Big Tech is able to promote a global standard of light-touch or no regulation.

43 Computer & Communications Industry Association Comment to USTR for 2023 NTE, Oct. 28, 2022. Available at: https://www.regulations.gov/comment/USTR-2022-0013-0047.

Commerce Secretary Gina Raimondo's public criticism of Europe's DMA[44] already has been leveraged to try to undermine similar legislative proposals making their way through Congress. For instance, the U.S. Chamber of Commerce argued that "*the White House needs to read its own talking points [regarding the DMA], before it takes a final position on the legislation [the American Innovation and Choice Online Act]. Providing support for similarly misguided domestic bills, the administration could transform the world's most innovative economy into one that reeks of stagnation*."[45]

The U.S. government revising its past position and not allowing, much less promoting, the broad anti-discrimination language in any future agreements is critical to countering Big Tech monopolies, something polling shows is among the few issues on which Americans across the political spectrum agree, which may explain why it also is a priority of the Biden administration and a growing bipartisan bloc in Congress.

CONCLUSION

It is critical to understand that the agenda that Big Tech has misbranded as "digital trade" is not focused on fixing real problems related to the online sale of imported goods. For example, today more than two million packages of online-purchased goods enter the U.S., mainly from China, daily without inspection and dodging taxes thanks to what is called the de minimis loophole in U.S. customs law. That is a real problem. Instead, Big Tech interests are trying to undermine policies that constrain entities' size or market power and promote fair competition, and civil rights, privacy and liability policies being promoted by the Biden administration and many in Congress from both parties – and by other governments worldwide.

The bottom line is that the USMCA and related TPP digital rules that represent the agenda promoted by Big Tech interests must not become the model or starting text for future agreements. And indeed, the provisions in the few existing pacts that include such rules must be revised to ensure countries' ability to adopt the effective policies required to ensure the health of both our economy and democracy in a digital age.

44 Jorge Liboreiro, "EU and US vow to boost microchip supplies and promote trustworthy AI," Euronews, Jan. 10, 2021. Available at: https://www.euronews.com/my-europe/2021/09/30/eu-and-us-vow-to-boost-microchip-supplies-and-promote-trustworthy-ai.

45 "Striking Similarities: Comparing Europe's Digital Markets Act to the American Innovation and Choice Online Act," U.S. Chamber of Commerce, Jun. 17, 2022. Available at: https://www.uschamber.com/finance/antitrust/striking-similarities-dma-american-innovation-act.

rethink TRADE

AMERICAN ECONOMIC LIBERTIES PROJECT

Undermining AI Regulation in the U.S. and Abroad: The "Digital Trade" Secrecy Ploy

July 2023

DIGITAL TRADE BRIEFING PAPERS SERIES #2

RETHINK TRADE

rethinktrade.org

Introduction

The development of artificial intelligence (AI) technologies, the evolution of the internet, and the growth of the data economy are fundamentally transforming every aspect of our lives. AI technologies can lead to more efficient exchanges and decision making. Yet unchecked and unregulated use of AI has proven to be harmful: It enables biased policing and prosecution, employment discrimination, intrusive worker surveillance, and unfair lending practices. Huge corporations, like Google and Amazon, also use problematic algorithms to self-preference their products and services and crush business competitors, increasing their monopoly power. In the United States and around the world, governments seek to seize the benefits of the digital revolution while also countering tech firms' ability to abuse workers, consumers, and smaller businesses.

In response, these powerful corporations are fighting back relentlessly. One under-the-radar strategy involves trying to lock in binding international rules that limit, if not altogether ban, key aspects of government oversight or regulation of the digital economy. To accomplish this, the tech industry is seeking to commandeer trade negotiations and establish what it calls "digital trade" agreements that would undermine Congress' and U.S. agencies' abilities to rein in their abuses.[1]

A key goal of industry's "digital trade" agenda is imposing rules that thwart governments from being able to proactively monitor, investigate, review, or screen AI and algorithms by forbidding government access to source code and perhaps, even detailed descriptions of algorithms.

Supporters of such source code and algorithm secrecy guarantees argue this is necessary to prevent untrustworthy governments from demanding tech firms hand over their algorithms, perhaps to be passed on to local companies that will knock off their inventions. That governments engaged in such conduct would be disciplined by new rules seems unlikely. Existing World Trade Organization (WTO) obligations and many nations' domestic laws already require governments to provide copyright protections and guarantees against disclosure of companies' confidential business information, including software's source code and other algorithmic data.[2] Businesses often complain that countries such as China do not comply with the existing rules.

Instead, these digital trade secrecy guarantees would bind scores of democratic countries worldwide that are considering new rules to prescreen or otherwise review the algorithms and source code running artificial intelligence applications in sensitive sectors. That industry's real goal is foreclosing AI regulation is underscored by the fact that the countries currently involved in U.S.-led trade negotiations do not have policies in place or under consideration that require government access to or transfer of source code or proprietary algorithms, according to a 2023 U.S. government review.[3]

1 David Dayen, "Big Tech Lobbyists Explain How They Took Over Washington," The American Prospect, 18 Apr. 2023. Available at: https://prospect.org/power/2023-04-18-big-tech-lobbyists-took-over-washington/.

2 Ulla-Maija Mylly, "Preserving the Public Domain: Limits on Overlapping Copyright and Trade Secret Protection of Software,". IIC 52, 1314–1337 (2021). Available at: https://doi.org/10.1007/s40319-021-01120-3.

3 Regarding countries involved in the Indo-Pacific Economic Framework Negotiations, see: Rethink Trade, "What Industry Identified as "Digital Trade Barriers" in the Indo-Pacific Region as Part of the National Trade Estimate Report Process," 17 Apr. 2023. Neither Kenya or Taiwan nor any Latin American or Caribbean country has imposed or is considering imposing this type of requirements according to the 2023 National Trade Estimate report. See: United States Trade Representative, 2023 National Trade Estimate Report on Foreign Trade Barriers. Available at: https://ustr.gov/sites/default/files/2023-03/2023%20NTE%20Report.pdf.

The primary effect of limiting governments' ability to demand source code and algorithm disclosure, then, would be to place the tech industry above regulatory oversight.

Casting a secrecy veil over source code and algorithms is especially problematic now that policymakers are responding to a growing movement demanding algorithmic transparency and accountability. The goal is for governments not only to have the tools to be able to sanction AI providers *after* their algorithms have been found to violate the law, but to *prevent* discriminatory or abusive practices. To do so, many AI experts have recommended policies that enable effective third-party audits of AI systems and/or require governmental pre-market screening conditioned upon access to source code and/or other types of algorithmic information particularly for high-risk sectors, like health services, credit, education, or employment.[4]

The European Union's Artificial Intelligence Act would, require firms to conduct conformity assessments prior to introducing high-risk AI applications to the European market to verify that the technology complies with the forthcoming regulation, in addition to prohibiting certain AI systems deemed to pose unacceptable risks to people's basic rights.

Under the EU policy, which is now being discussed by the European institutions, high-risk AI systems include those that can create risks for the health and safety or fundamental rights of natural persons, such as those related to critical infrastructure, education or employment, eligibility for public benefits, and credit scoring. National supervisory agencies in each EU member country

What is AI?

We hear the term "AI" everywhere.

And the use of AI is pervasive. But what is it exactly?

Although often associated with the simulation of human "intelligence," AI is a loosely defined term used to describe a wide spectrum of data-driven technologies that are often used to aid or replace human decision-making or provide recommendations and predictions.

Recently, generative AI, a technology that creates content such as text or video by identifying patterns in large quantities of training data, has received significant public attention.

Yet other AI-powered tools, commonly referred to as automated decision systems (ADS), are much more widely used and until now have a larger impact on everyone's daily lives. Decisions around hiring and workplace management, whether an applicant gets a home loan or insurance coverage, and peoples' access to public and private services, amongst many other areas, increasingly rely on ADS.

Underpinning these AI systems are a few core elements: large amounts of data, algorithms that process such data towards specific objectives, and computational power providing the infrastructure for such processing. The algorithm, expressed in a way that humans can understand it, is an example of "source code."

AI systems in practice have resulted in a range of demonstrated harms including inaccuracies, or biases that disproportionately affect particular demographic groups, such as women, people of color, or people with disabilities. These biases often stem from decisions around the type of data the model has been trained on, or the design of the algorithmic model itself, as embedded in its source code.

4 Timnit Gebru, Emily M. Bender, Angelina McMillan-Major, and Margaret Mitchell, "Statement from the listed authors of Stochastic Parrots on the "AI pause" letter," 31 Mar. 2023. Available at: https://www.dair-institute.org/blog/letter-statement-March2023; Data Ethics Commission, "Opinion of the Data Ethics Commission," 2019. P. 19, 184 Available at: https://www.bmj.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN.pdf?__blob=publicationFile&v=2; Emanuel Moss, et al, "Assembling Accountability, Data & Society," Data & Society, 29 Jun. 2021. Available at: https://datasociety.net/library/assembling-accountability-algorithmic-impact-assessment-for-the-public-interest/; Kristina Irion, "AI Regulation in the European Union and Trade Law: How Can Accountability of AI and a High Level of Consumer Protection Prevail over a Trade Discipline on Source Code?" (26 Jan. 2021). Available at SSRN: https://ssrn.com/abstract=3786567 or http://dx.doi.org/10.2139/ssrn.3786567.

were to have access to all information necessary to enforce the law, including source code.[5] However, a recent investigation revealed that EU trade authorities demanded that the Commission's proposal be weakened, so as to comply with source code secrecy rules that the EU negotiated with the United Kingdom.[6] The changes restrict the capacity of national supervisory agencies and external auditors to access the source code of high-risk AI applications.

In the United States, the House Committee on Energy and Commerce approved the American Data Privacy and Protection Act (ADPPA) on July 20, 2022, by a large bipartisan majority.[7] ADPPA is expected to be reintroduced in the current Congress. If enacted, this legislation would be the first U.S. national policy protecting personal data. Importantly, the ADPPA also includes a "civil rights and algorithms" title, which requires that certain entities submit impact assessments and algorithm design evaluations to the Federal Trade Commission (FTC).[8]

This bill is part of a broader strategy to ensure tech accountability in the United States. In October 2022, the White House released a document called "The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People." This document is intended to support the development of policies and practices that protect civil rights and promote democratic values in the building, deployment, and governance of automated systems. The blueprint calls for pre-deployment testing, risk identification and mitigation, and ongoing monitoring to ensure that AI systems are not unsafe, discriminatory, inaccurate, or ineffective. It calls for this to be confirmed by independent evaluation though algorithmic impact assessments.[9] Some AI experts have lamented the non-binding nature of the Blueprint.[10] However, even the possibility of third-party evaluations triggered the U.S. Chamber of Commerce to send a letter to the White House criticizing the proposal.[11]

To effectively implement the oversight needed to promote AI accountability or algorithmic justice, U.S. regulators and courts must have the ability to gain access to information about companies' AI systems, including source code and the data being fed into the program.

---

5 Mark MacCarthy and Kenneth Propp, "Machines learn that Brussels writes the rules: The EU's new AI regulation." Brookings, 4 May 2021. Available at: https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/; Art. 64.2 of the Artificial Intelligence Act proposal: "Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2 and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system." Accessed on 13 Dec. 2022. Available at: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.

6 Mark MacCarthy and Kenneth Propp, "Machines learn that Brussels writes the rules: The EU's new AI regulation." Brookings, 4 May 2021. Available at: https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/; Art. 64.2 of the Artificial Intelligence Act proposal: "Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2 and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system." Accessed on 13 Dec. 2022. Available at: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.

7 Aysha F. Allos, "American Data Privacy and Protection Act: Are We Finally Getting Federal Data Privacy Protection?" The National Law Review, 21 Sept. 2022. Available at: https://www.natlawreview.com/article/american-data-privacy-and-protection-act-are-we-finally-getting-federal-data-privacy.

8 Section 207(c) of the American Data Privacy and Protection Act (ADPPA). Accessed on 25 Sept. 2022. Available at: https://www.congress.gov/bill/117th-congress/house-bill/8152/text#toc-H6332551148B14109B1F2D9598E099E38.

9 White House, Office of Science and Technology Policy, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People. Available at: https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

10 Khari Johnson, "Biden's AI Bill of Rights is Toothless Against Big Tech," Wired, 4 Oct. 2022. Available at: https://www.wired.com/story/bidens-ai-bill-of-rights-is-toothless-against-big-tech/.

11 Derek Robertson, "Some signs that Meta may be playing nice," Politico, 12 Oct. 2022. Available at: https://www.politico.com/newsletters/digital-future-daily/2022/10/12/some-signs-that-meta-may-be-playing-nice-00061504.

Casting a secrecy veil over source code and algorithms is especially problematic now that policymakers are responding to a growing movement demanding algorithmic transparency and accountability.

However, tech interests both are trying to water down regulation at home,[12] while also pushing for "digital trade" provisions that explicitly forbid governments from having access to review software source code or algorithms, save for a few exceptions related to certain agencies and related to specific investigations or known problems.[13] In the most recent U.S. trade deal, the United States-Mexico-Canada Agreement (USMCA), these interests managed to insert prohibition on government access for not only source code, but also algorithms as a whole.[14]

Bournemouth University's legal scholars Maurizio Borghi and Benjamin White have pointed out that, given USMCA's broad definition of 'algorithms,'[15] this disclosure prohibition potentially covers descriptions of algorithms, not only the detailed source code developed by programmers.[16] This problematic, broad obligation and the secrecy protections it would impose could then preclude even the less expansive prescreening requirements proposed to date, like the one included in the ADPPA.[17]

Very few "digital trade" or e-commerce agreements have such extreme provisions. Only 11 of the 181 agreements with digital trade or e-commerce terms include secrecy guarantees for source code according to a trade-pact database that runs through mid-2021.[18] But tech interests hope to use Indo-Pacific Economic Framework (IPEF) negotiations now underway to impose such constraints on the governments that make up more than 40% of the world economy and do the same to the nations involved in the Americas Partnership for Economic Prosperity (APEP) negotiations. By doing so, they hope to "normalize" what are extreme and rare trade-agreement-imposed constraints on AI regulation, and perhaps get such terms inserted into a global agreement some countries are trying to negotiate called the Joint Statement Initiative on E-Commerce.

12 Emily Birnbaum, "The AI 'gold rush' in Washington," Politico, 29 Jun. 2022. Available at: https://www.politico.com/newsletters/digital-future-daily/2022/06/29/small-fry-ai-dc-try-00043278.

13 Third World Network Briefings, op. cit; International Trade Union Confederation, E-Commerce Free Trade Agreements, Digital Chapters and the Impact on Labour. (London, 2019), 4. Available at: https://www.ituc-csi.org/e-commerce-report.

14 USMCA Article 19.16.1 states: "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."

15 USMCA Article 19.1 states: "algorithm means a defined sequence of steps, taken to solve a problem or obtain a result."

16 Maurizio Borghi and Benjamin White, "Data extractivism and public access to algorithms: Mapping the battleground of international digital trade", in Law, Regulation and Governance in the Information Society. London, Routledge, 2022. P. 116.

17 ADPPA Section 207(c)(B) states: "The impact assessment required under subparagraph (A) shall provide the following: (i) A detailed description of the design process and methodologies of the covered algorithm (...)." Accessed on 25 Sept. 2022. Available at: https://www.congress.gov/bill/117th-congress/house-bill/8152/text#toc-H6332551148B14109B1F2D9598E099E38.

18 Calculations made using the TAPED dataset, "The Governance of Big Data in Trade Agreements," Universities of Lucerne and Bern. Accessed on Oct. 3, 2022. Available at: https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-directorinternationalisation/research/taped/.

The chart below shows the horizontal policies (meaning those that apply to multiple sectors and domains), and the area-specific policies that would be undercut by including secrecy guarantees for source code and algorithms in trade deals.

The rest of this Briefing Paper explores in detail some of the policy domains in which source code and algorithm secrecy guarantees could undermine existing government regulatory powers and derail future policies to counter AI-enabled abuses by tech companies.

Algorithmic Transparency and Accountability Policies Undercut by Source Code and Algorithm Secrecy Provisions

Horizontal Policies	White House Blueprint for an AI Bill of Rights American Data Privacy and Protection Act (ADPPA) Rules on Civil Rights and Algorithms Algorithmic Accountability Act of 2019			
	Area-Specific Policies			
	Criminal Justice System and Law Enforcement	**Fair Lending and Housing**	**Labor and Employment Law**	**Anti-Monopoly and Competition Policy**
Federal	Justice in Forensic Algorithms Act of 2021 Facial Recognition and Biometric Technology Moratorium Act of 2023 Facial Recognition Act of 2022	Biden Administration's Rulemaking on Property Appraisal and Valuation Equity Obama Administration's Report on Algorithmic Systems, Opportunity, and Civil Rights	Stop Spying Bosses Act of 2023	Department of Transportation's Algorithmic Disclosure Requirements for Computer Reservation Systems (CRS)**
State	Idaho's Criminal Procedure Rule on Pretrial Risk Assessments*			
	Washington's Guidelines on Government Procurement and Use of Automated Decision Systems			
Local	Washington D.C.'s 2023 Stop Discrimination by Algorithms Act			

* This legislation is already in force in the state of Idaho.

** This regulation expired in 2004.

Source Code Secrecy Protections Can Prevent Efforts to Regulate AI Use and Abuse in the Criminal Justice System

AI is being employed in the criminal justice system, with potentially untold dangerous consequences. From policing to investigation and trials to sentencing, the U.S. criminal justice system is increasingly becoming automated. While inaccurate or biased AI poses threats in many uses, the stakes are particularly high when people's liberty and lives are involved.

Yet law enforcement agencies have unreservedly embraced the use of forensic algorithms when investigating potential crimes and submitting evidence to court. There are three main types of forensic algorithms: facial recognition software, latent prints programs to identify finger and palm prints, and probabilistic genotyping. (Genotyping AI uses DNA samples from a crime scene and through statistical methods and mathematical algorithms compares them to a reference profile from one or more persons of interest.)[19]

AI is presented as infallible to judges and juries. And, when defense counsel seeks to examine forensic algorithm tools and access the source code and underlying data to challenge the evidence being brought against defendants, sometimes developers of these programs have used trade secrets law to block access and scrutiny. In order to contribute to defendants' right to a fair trial, Rep. Mark Takano (D-Calif.) introduced H.R. 2438: the Justice in Forensic Algorithms Act of 2021, which would prohibit the use of trade secrets law to block criminal defense scrutiny of law enforcement technologies, such as forensic algorithms. The legislation would also: (i) require the National Institute of Standards and Technology (NIST) to develop standards for testing computational forensic software; (ii) create a Computational Forensic Algorithm Testing Program at NIST, which would be in charge of testing software; and (iii) require that federal law enforcement agencies could only use forensic software that has been tested and approved by NIST. Finally, the bill requires that defendants are granted access to both the source code for the version of the computational forensic software used in their case and any relevant data used to train the algorithm.[20]

19 'Forensic algorithms: The future of technology in the US legal system,' Brookings Event. 12 May 2022. Video available at: https://www.brookings.edu/events/forensic-algorithms-the-future-of-technology-in-the-us-legal-system/.

20 H.R.2438 - Justice in Forensic Algorithms Act of 2021. Available at: https://www.congress.gov/bill/117th-congress/house-bill/2438/text.

Senators Edward Markey (D-Mass.) and Jeff Merkley (D-Oreg.) and Rep. Pramila Jayapal (D-Wash.) lead a bicameral group of Democrats proposing S. 2052/H.R.3907: the Facial Recognition and Biometric Technology Moratorium Act. This legislation would prevent federal agencies from using facial recognition and other biometric technologies, unless certain conditions are met, including the adoption of auditing requirements to ensure accuracy.[21] Reps. Ted Lieu (D-Calif.), Sheila Jackson Lee (D-Tex.), Yvette Clarke (D-NY), and Jimmy Gomez (D-Calif.) proposed H.R. 9061, the Facial Recognition Act of 2022, which limits use of facial recognition software to cases where law enforcement has obtained a warrant and bans its use to track individuals with live or stored video footage. Importantly, the bill would also require regular auditing of facial recognition systems used by law enforcement agencies and suspensions for agencies that fail audits, plus annual independent testing of any facial recognition software that law enforcement employs.[22]

It is easy to see how the different elements of these proposals are in direct contradiction with tech industry's trade-pact demand for expansive secrecy guarantees for source code. And contrary to claims by tech interests, the exceptions included in the past few pacts that included such secrecy terms do not fix the problem. The exceptions do not cover criminal justice AI uses, but rather focus on critical infrastructure, competition law, and intellectual property, or only cover orders from a regulatory body or court requiring source code disclosure for specific investigations and to a regulatory body, not allowing source code access by courts or a defendant in a criminal case, as proposed by Rep. Takano's bill.[23]

Another problematic use of AI in the criminal system is for risk assessments. Risk assessments are employed in a myriad of ways, from setting a defendants' bail[24] to judging their eligibility for alternative rehabilitative treatment[25] to determining the conditions of their probation,[26] to – in some states – sentencing by mandating the amount of prison time a defendant must serve.[27] However, these forecasting assessment tools rely on algorithms that are potentially fed biased and inaccurate data.

21 Office of Representative Ed Markey, 'Markey, Merkley, Jayapal Lead Colleagues on Legislation to Ban Government Use of Facial Recognition and Other Biometric Technology,' 7 Mar. 2023. Available at: https://www.markey.senate.gov/news/press-releases/markey-merkley-jayapal-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-and-other-biometric-technology.

22 Office of Representative Ted Lieu, 'Reps Ted Lieu, Sheila Jackson Lee, Yvette Clarke, and Jimmy Gomez Introduce Bill to Regulate Law Enforcement Use of Facial Recognition Technology,' 29 Sept. 2022. Available at: https://lieu.house.gov/media-center/press-releases/reps-ted-lieu-sheila-jackson-lee-yvette-clarke-and-jimmy-gomez-introduce.

23 USMCA Article 19.16.2 states: "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, subject to safeguards against unauthorized disclosure."

24 Anna Maria Barry-Jester et. al., "The New Science of Sentencing," The Marshall Project, 4 Aug. 2015. Available at: https://www.themarshallproject.org/2015/08/04/the-new-science-of-sentencing.

25 Julia Angwin et al., "Machine Bias," ProPublica, 23 May 2016. Available at: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. See also Kate Crawford, "Artificial Intelligence's White Guy Problem," New York Times, 26 Jun. 2016. Available at: https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html?mcubz=1.

26 Eileen Sullivan et al., "States predict inmates' future crimes with secretive surveys," Associated Press, 24 Feb. 2015. Available at: https://apnews.com/article/027a00d70782476eb7cd07fbcca40fc2.

27 Alexandra Chouldekova, "Fair Prediction with Disparate Impact: A Study of Bias in Recidivism Prediction Instruments," Updated Feb. 2017, https://arxiv.org/pdf/1703.00056.pdf.

Risk assessment algorithms are informed by questionnaires, which ask about a defendant's education, job status, family, income, parents' involvement with the criminal justice system, and even whether they have a phone. This information constructs a score. The scores are based on previous offenders' behavior who responded similarly to a current defendant. Risk corresponds to the score – if the score is higher, the defendant is deemed higher risk and faces more scrutiny and monitoring.

This model to predict recidivism has been criticized for potentially overpredicting the chance that Black defendants would commit another crime. By relying on data about past offenders to predict what current and future defendants might do after being released from prison, these algorithms reinforce existing racial disparities in the criminal justice system.

A ProPublica study, based on 7,000 risks scores found in Broward County in Florida, concluded that the algorithm was neither reliable nor accurate and exhibited significant racial biases. Only 20% of the people predicted to commit violent crimes by the risk assessment system actually went on to do so. Plus, the algorithm used in that county was likely to flag Black defendants as future defendants at almost twice the rate as white defendants. White defendants were mislabeled as low risk more often than Black defendants.[28]

The parties making the risk assessment software do not publicly disclose the specific process behind how scores are generated. Defendants are unable to challenge these assessments, and they also are not privy to the data calculations. Even judges are unable to understand the logic behind the software. [29]

28 Angwin et al., op. cit.

29 Crawford, et al., op. cit.

According to Professor Christopher Slobogin, director of the criminal justice program at Vanderbilt Law School, "*risk assessments should be impermissible unless both parties get to see all the data that go into them. It should be an open, full-court adversarial proceeding.*"[30] In 2019, Idaho enacted a policy consistent with Professor Slobogin's recommendation. It requires that any pretrial risk assessment must be shown to be non-discriminatory before being used and localities availing themselves of these tools must guarantee that all documents, records, and information used to build or validate the risk assessment are open to public inspection, auditing, and testing.[31] The risk assessment system's source code is part of the information that would be required by a defendant to be able to exercise their right to due process, as well as part of the documentation that Idaho requires to be publicly available. Yet, the source code secrecy terms that tech industry interests seek in "digital trade" agreements would deny access to such information.

AI's role in the criminal system has not been limited to the courtroom. Police departments across the United States are also using data-driven risk-assessment tools in "predictive policing" crime prevention efforts. In many cities, including New York, Los Angeles, San Francisco, Chicago, and St. Louis, software analyses of large sets of historical crime data are used to identify crime "hot spots." The police then aggressively patrol these areas with the objective of deterring crime before it happens.[32]

> The widespread use of 'predictive policing' software, risk assessments systems, forensic algorithms, and the general pervasiveness of AI systems in public administration has fueled claims in many U.S. states for transparency rules at the local government level.

Civil liberties advocates have raised concerns about such software potentially perpetuating a vicious cycle: The police increase their presence in the same places they are already policing, thus ensuring that more arrests come from those areas, which dooms these places as crime "hot spots."[33] Additionally, predictive programs are only as good as the data on which they are trained, and that data has a complex history. A recent study from researchers from the AI Now Institute at New York University shows that the data used by these systems in several jurisdictions were produced during documented periods of flawed, racially biased, and sometimes unlawful policing practices and policies. Basing predictive policing on this "dirty data" risks entrenching the practices that have led to unlawful and biased policing practices.[34]

30 Angwin et al., op. cit.

31 Idaho Legislature. House Bill 118. Jul. 1, 2019. Accessed 8 Dec. 2022. Available at: https://legislature.idaho.gov/sessioninfo/2019/legislation/H0118/.

32 Maurice Chammah, "Policing the Future," The Marshall Project, 3 Feb. 2016. Available at: https://www.themarshallproject.org/2016/02/03/policing-the-future#.9vrCo3ZOH; Andrew Guthrie Ferguson, "Predicting Predictive Policing in NYC," Huffington Post, 8 Jul. 2016. Available at: https://www.huffpost.com/entry/predicting-predictive-pol_b_7757200; Darwin Bond-Graham and Ali Winston, "All Tomorrow's Crimes: The Future of Policing Looks a Lot Like Good Branding," SF Weekly, 30 Oct. 2013. Available at: https://archives.sfweekly.com/sanfrancisco/all-tomorrows-crimes-the-future-of-policing-looks-a-lot-like-good-branding/Content?oid=2827968.

33 Chammah, op. cit.

34 Rashida Richardson, Jason Schultz, and Kate Crawford, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," (13 Feb. 2019). 94 N.Y.U. L. REV. ONLINE 192 (2019), Available at SSRN: https://ssrn.com/abstract=3333423.

The widespread use of "predictive policing" software, risk assessments systems, forensic algorithms, and the general pervasiveness of AI systems in public administration has fueled claims in many U.S. states for transparency rules at the local government level. These rules would guarantee public access to software's source code of automated decision systems (ADS) employed by local authorities.

The policies being advanced to address these concerns reflect the audit and review tools included in the Biden administration's Blueprint for an AI Bill of Rights. New York City established an ADS Task Force, consisting of a group of city officials assigned with the responsibility to establish a process for reviewing the city's use of automated decision systems. In 2018, a group of AI experts wrote a report in parallel with the Task Force, recommending that the city release a public list of ADS used by agencies both online and accessible in print at branches of the New York Public Library system. They called for this list to include, among other information, ADS' source code.[35] In Washington, state legislators introduced a bill in 2021 that would require state agencies to ensure that ADS vendors make both the system and data used to develop the algorithm freely available for agency or third-party testing, auditing, and research, while also prohibiting non-disclosure clauses that would preclude access to algorithmic information.[36] The Electronic Privacy Information Center (EPIC) published a report documenting the generalized used of ADS in Washington D.C. that showed at least 20 agencies use 29 systems. EPIC recommended, among other policies, enacting laws requiring comprehensive algorithmic governance, including audits and impact assessments.[37] This recommendation is consistent with the 2023 Stop Discrimination by Algorithms Act proposed by former D.C. Attorney General Karl Racine, a bill requiring companies to audit their algorithms for discriminatory patterns and submit annual reports to the Office of the Attorney General for the District of Columbia with information including the methodologies and optimization criteria of the algorithms.[38]

These policies would likely run afoul of the extreme source code secrecy guarantees that the tech industry seeks in IPEF and other digital trade deals. While most existing digital trade deals have carveouts for government procurement, it is unlikely that the types of policies described above would qualify for this reservation. USMCA, for instance, defines government procurement as *"the process by which a government obtains the use of or acquires goods or services (…) for governmental purposes (…)."* By emphasizing on the procurement "process," the carveout likely only covers the conditions that agencies can adopt when carrying out a public tender or negotiating a government contract. This would leave policies that create general conditions for AI systems that government can use or those that would make public ADS purchased by local governments susceptible to attacks based on source code secrecy guarantees.

35 Rashida Richardson, ed., "Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force," AI Now Institute, 4 Dec. 2019. Available at: https://ainowinstitute.org/publication/confronting-black-boxes-a-shadow-report-of-the-new-york-city-automated.

36 Washington Legislature. SB 5116 - 2021-22: Establishing guidelines for government procurement and use of automated decision systems in order to protect consumers, improve transparency, and create more market predictability. Accessed on 7 Dec. 2022. Available at: https://app.leg.wa.gov/billsummary?billnumber=5116&year=2021&msclkid=7dc3be5fc26c11ecb582ea23e6e5b75d#documentSection.

37 Electronic Privacy Information Center, "Screened & Scored in D.C.," Nov. 2022. Available at: https://epic.org/screened-scored-in-dc/.

38 Office of the Attorney General for the District of Columbia, 'AG Racine Introduces Legislation to Stop Discrimination In Automated Decision-Making Tools That Impact Individuals' Daily Lives,' 9 Dec. 2021. Available at: https://oag.dc.gov/release/ag-racine-introduces-legislation-stop.

Source Code Secrecy Protections Can Obstruct Efforts to Guarantee Fair Lending and Housing

Statistical models and algorithms have been used in consumer finance for decades to provide information for loan officers to consider. However, today's systems are being used in unprecedented ways to decide who will gain access to a home loan or other types of credit and under which terms, with very little human oversight or input.

The extensive use of such AI in consumer finance is controversial, as it is likely to entrench or even worsen the long-standing discrimination that minorities face in credit markets. A 2021 study found that lenders were 40 to 90% more likely to turn down Latino, Asian, Native American, and Black applicants than similar white applicants. Black applicants in higher income brackets with less debt were rejected more often than white applicants in the same income bracket, who had more debt.[39] Another study found that borrowers from minority groups were charged interest rates that were nearly 8% higher than their white counterparts.[40]

When huge datasets are used to analyze creditworthiness, certain variables – such as level of education – could act as proxies for race, ethnicity, or gender, allowing AI systems to systematically determine that, for instance, Black or Latino applicants are less creditworthy than white people.[41] And, if wealth is used as a barrier to entry, white people are automatically favored, given that at present, white families typically hold eight times the wealth of typical Black families.[42] Plus, the type of data collected and/or the exclusion of data is troubling and prevalent. Decades of bias in credit decisions means different amounts of data are available in the credit histories of different categories of people. The absence of data has been shown to result in different mortgage approval rates between minority and majority applicants.[43]

This data is then fed into automated decision systems that employ algorithms that often have disproportionately negative effects on communities of color because they reflect the unequal access to credit that resulted from America's long history of discrimination.

Consider the classic FICO credit model as a way to understand how both data and design problems can result in discriminatory outcomes. This credit scoring algorithm is used by many big lenders, such as the Federal National Mortgage Association (Fannie Mae) and the Federal Home Loan

39 Emmanuel Martinez, et al., "The Secret Bias Hidden in Mortgage-Approval Algorithms", The Markup, 25 Aug. 2021. Available at: https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

40 Robert Barlett, Adair Morse, Richard Stanton, and Nancy Wallace, "Consumer-lending discrimination in the FinTech Era," Journal of Financial Economics, Vol. 143, No. 1. Jan. 2022. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0304405X21002403?via%3Dihub.

41 Carol Evans, et al., "Keeping Fintech Fair: Thinking About Fair Lending and UNDAP risks", Computer Compliance Outlook, Second Issue 2017. Available at: https://www.consumercomplianceoutlook.org/2017/second-issue/keeping-fintech-fair-thinking-about-fair-lending-and-udap-risks/.

42 David Brancaccio, "How mortgage algorithms perpetuate racial disparity in home lending", Marketplace, 25 Aug 2021. Available at: https://www.marketplace.org/2021/08/25/housing-mortgage-algorithms-racial-disparities-bias-home-lending/.

43 Will Douglas Heaven, "Bias isn't the only problem with credit scores – and no, AI can't help," MIT Technology Review, 17 Jun. 2021. Available at: https://www.technologyreview.com/2021/06/17/1026519/racial-bias-noisy-data-credit-scores-mortgage-loans-fairness-machine-learning/.

Mortgage Corporation (Freddie Mac), to assess and decide mortgage applications. The Classic FICO algorithm was built using data from the 1990s and is more than fifteen years old. It only considers traditional credit, which is more accessible to white Americans, and does not account for timely rent and telephone bill payments. (It does capture late payments of rent and phone bills as demerits.) FICO will only assign a credit score for people who meet certain minimum scoring criteria, such as having a bank account open for more than six months.

Discriminating on the base of gender, race, or ethnicity is already banned by the Equal Credit Opportunity Act and the Fair Housing Act. However, these statutes are underenforced. Lack of access to the underlying source code is a contributing factor.

To counter such bias, experts have recommended creating fairer credit models or using alternatives. Vantage Score is one example of a credit model competing with FICO. It does not limit the pool of people that can have a credit score via the sort of minimum scoring criteria used in FICO. Vantage reports that it can provide 37 million Americans with credit who currently have no FICO score, a third of whom are Black or Latino.[44] Creating a more inclusive credit rating model would involve the related AI systems omitting data on crime, schools, and income, which in turn would better protect people's ethnicity and race from being disclosed.[45] More accurate metrics to measure risk, such as crediting timely rent and utility payments, would allow mortgage lenders to choose applicants based on their ability to pay back a loan without enforcing historically discriminatory trends.

Discriminating on the base of gender, race, or ethnicity is already banned by the Equal Credit Opportunity Act and the Fair Housing Act. However, these statutes are underenforced.[46] Lack of access to the underlying source code is a contributing factor. Already in 2016, the Obama administration recommended promoting algorithmic auditing and external testing of big data systems to ensure that people are being treated fairly.[47] This recommendation was partially based on already existing concerns about credit eligibility decisions being made by algorithms that have the potential to perpetuate, exacerbate, or mask discrimination. In turn, the Biden administration has committed to include a non-discrimination standard in a forthcoming regulation on automated valuation models used to determine the collateral worth of a mortgage secured by the lender's house.[48] Enforcing the compliance with such a non-discrimination standard would require permitting agencies to have access to these models' source code and underlying data. Yet "digital trade" provisions that ban access to source code and algorithms would be in direct contradictions with these policies.

---

44 Martinez et al., op cit.

45 Tony Cantu, "How one firm is overcoming racial bias in the mortgage industry," Mortgage Professional America Magazine, 10 Dec. 2021. Available at: https://www.mpamag.com/us/news/general/how-one-firm-is-overcoming-racial-bias-in-the-mortgage-industry/319520.

46 Martinez et al., op cit.

47 White House, "Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights," May 2016. P. 23. Available at: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

48 Interagency Task Force on Property Appraisal and Valuation Equity, "Action Plan to Advance Property Appraisal and Valuation Equity: Closing the Racial Wealth Gap by Addressing Mis-valuations for Families and Communities of Color," Mar. 2022. P. 27. Available at: https://pave.hud.gov/sites/pave.hud.gov/files/documents/PAVEActionPlan.pdf.

Source Code Secrecy Can Conceal Labor Law Violations and Employment Discrimination

When it comes to work, AI-enabled digital technologies are being used by employers to recruit, hire, and evaluate the performance of — and exert control over — workers. AI is also being used to partially automate tasks in the name of increasing productivity, by getting more done with fewer people.[49] The use of digital technologies in the workplace doesn't need to hurt workers. However, the unchecked and unregulated usage of AI technologies by employers can easily lead to violations of wage and hour labor laws with work speed-ups and scheduling gimmicks that result in people working when not 'on the clock' and not being paid.

The use of digital technologies in the workplace doesn't need to hurt workers. However, the unchecked and unregulated usage of AI technologies by employers can easily lead to violations of wage and hour labor laws with work speed-ups and scheduling gimmicks that result in people working when not 'on the clock' and not being paid.

For instance, in 2015, workers filed class-action lawsuits against McDonald's stores in California, Michigan, and New York, alleging systematic wage theft associated with workplace management software. The stores involved reportedly used a computer program that calculated labor costs every fifteen minutes as a percentage of revenue. When the labor cost share was above a predetermined target, managers would routinely order employees to clock out and wait in break rooms for minutes or hours without pay. Only when revenue picked up were workers allowed to clock back in. Managers would tell workers to clock out before the end of their shifts but insist that they finish certain tasks before going home.[50]

AI programs also undermine workers' rights to organize unions and foster hazardous working conditions, growth in contingent work, and loss of autonomy and privacy.[51] AI-enabled surveillance technologies already have been used by companies like Walmart, Amazon, Google, and HelloFresh with the intent of chilling union organizing. [52] Among other tactics, these firms have monitored employees' activity, conversations, and social media posts about union activism. Employers have used heat maps, which were based on predictive analytics, to track store locations considered at high risk of union activity. They have also utilized systems to alert managers to any internal meetings scheduled with 100 or more employees.

49 Annette Bernhardt, Annette Kresge, and Reem Suleiman, "Data and Algorithms at Work; The Case for Worker Technology Rights." Berkeley: Center for Labor Research and Education, University of California, Berkeley. 3 Nov. 2021. P. 7. Available at: https://laborcenter.berkeley.edu/data-algorithms-at-work/.

50 Esther Kaplan, "The Spy Who Fired Me," Harper's Magazine, Mar. 2015. Available at: https://harpers.org/archive/2015/03/the-spy-who-fired-me/.

51 Bernhardt, Kresge & Suleiman, op cit. P. 16.

52 Jo Constantz, "'They Were Spying On Us': Amazon, Walmart, Use Surveillance Technology to Bust Unions", Newsweek, Dec. 2021. Available at: https://www.newsweek.com/they-were-spying-us-amazon-walmart-use-surveillance-technology-bust-unions-1658603".

Concerning hazardous working conditions, Amazon tracks and monitors warehouse workers' entire workday. Any "time-off-task," such as unallotted bathroom breaks, can generate algorithm-based warnings or even lead to termination.[53] This kind of workplace surveillance jeopardizes workers' safety. Ratcheting up workloads and work speeds have contributed to Amazon's injury rate, which is three times the national average and, for serious injuries, five times the national average.[54]

Additionally, algorithmic hiring and recruitment software can replicate and deepen existing inequities. Certain individuals are systematically excluded from employment when source code reflects the biases of its developers or when the algorithm is trained by inaccurate, biased, or unrepresentative data.[55] The Equal Employment Opportunity Commission is already investigating at least two cases involving claims that algorithms unlawfully exclude certain groups of workers during the recruitment process.[56] This is not a negligible issue: Major employers such as Unilever, Hilton, and Delta Air Lines use data-driven predictive hiring tools,[57] which inform decisions that could be exacerbating racial, ethnic, and gender inequalities.

To prevent workplace discrimination or sanction it if it occurs, violations of wage and hour laws, and the proliferation of hazardous working conditions, experts recommend adopting policies that require impact assessments or audits for regulatory investigations.[58] Requiring firms to conduct these impact assessments or audits to prevent labor law violations could be a policy to be adopted by the Privacy and Technology Division that S.262: the Stop Spying Bosses Act, a bill recently introduced by Senators Bob Casey (D-Pa.), Cory Booker (D-NJ), and Brian Schatz (D-Hawaii), would create at the Department of Labor to enforce and regulate workplace surveillance.[59] All of these would require access to software's algorithms and potentially source code, which digital firms are trying to preclude through obscure "digital trade" rules.

Guarantees of Source Code Secrecy Can Cloak Anti-Monopoly and Competition Policy Violations

Consumers were promised that the rise of online markets, underpinned by the data economy and powerful algorithms, would encourage competition and efficiency. Yet, behind the façade of virtual

53 Colin Lecher, "How Amazon automatically tracks and fires warehouse workers for 'productivity,'" The Verge, 25 Apr. 2019. Available at: https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations.

54 National Employment Law Project and The Athena Coalition, "Packaging Pain: Workplace Injuries in Amazon's Empire," Dec. 2019. P. 3. Available at: https://worker-centerlibrary.org/product/packaging-pain-workplace-injuries-in-amazons-empire/.

55 Jenny Yang, "The Future of Work: Protecting Workers' Civil Rights in the Digital Age, Before the Civil Rights and Human Services Subcommittee," 5 Feb. 2020. P. 5. Available at: https://www.congress.gov/116/meeting/house/110438/witnesses/HHRG-116-ED07-Wstate-YangJDJ-20200205.pdf.

56 Chris Opfer, "AI Hiring Could Mean Robot Discrimination Will Head to Courts," Bloomberg Law, Nov. 2019. Available at: https://news.bloomberglaw.com/daily-labor-report/ai-hiring-could-mean-robot-discrimination-will-head-to-courts.

57 Drew Harwell, "A face-scanning algorithm increasingly decides whether you deserve the job," Washington Post, 6 Nov. 2019. Available at: https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

58 Yang, op cit. P. 13; Bernhardt, Kresge & Suleiman, op cit. P. 25-26.

59 Office of Senator Casey, "Casey, Booker, Schatz Introduce Bill to Protect Workers from Invasive, Exploitative Surveillance Technologies," 2 Feb. 2023. Available at: https://www.casey.senate.gov/news/releases/casey-booker-schatz-introduce-bill-to-protect-workers-from-invasive-exploitative-surveillance-technologies.

competition, algorithms often hide collusive behavior, price discrimination, self-preferencing by the largest platforms, and other forms of monopolistic abuse that thwart the promised benefits and threaten the resilience of the wider economy. The public is seeing the evidence of such misconduct in press reports while policymakers also review scholarly research documenting how dominant platforms use AI to expand their monopoly power.

Yet, behind the façade of virtual competition, algorithms often hide collusive behavior, price discrimination, self-preferencing by the largest platforms, and other forms of monopolistic abuse that thwart the promised benefits and threaten the resilience of the wider economy.

Algorithms can further collusion among competitors either by acting as a "hub" that creates the scenario for competing firms to collude without being even in contact with each other or by providing means to monitor compliance with a human-made or AI-set price-fixing agreements.[60] The French and German governments' competition authorities identified the way in which algorithms can be used by firms to collude and charge higher prices on consumers in a joint report:

"Data collection may also facilitate collusion when these data are used to fix prices through the use of algorithms. Even though market transparency as a facilitating factor for collusion has been debated for several decades now, it gains new relevance due to technical developments such as sophisticated computer algorithms. For example, by processing all available information and thus monitoring and analysing or anticipating their competitors' responses to current and future prices, competitors may easier be able to find a sustainable supra-competitive price equilibrium which they can agree on."[61]

These are not hypothetical concerns. In 2015, the U.S. Department of Justice (DOJ) charged a group of sellers in the Amazon marketplace for fixing the prices of posters sold online between September 2013 and January 2014. According to the DOJ's investigation, the conspirators designed and shared among each other dynamic pricing algorithms that were programmed to coordinate changes to their respective prices.[62] In November 2022, a group of renters filed a lawsuit against RealPage and nine big property managers for allegedly forming a cartel to artificially inflate rents through RealPage's price-setting software for apartments.[63] Two additional lawsuits were filed against RealPage since then, and several lawmakers have called on the FTC and DOJ to investigate RealPage's rent-setting software.[64]

---

60 Competition & Markets Authority, "Pricing algorithms: Economic working paper on the use of algorithms to facilitate collusion and personalised pricing," 8 Oct. 2018. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_report.pdf; Ariel Ezrachi, and Maurice Stucke, Virtual Competition: The Promise and Perils of the Algorithmic-Driven Economy. Cambridge, Massachusetts, Harvard University Press, 2016. P. 35 – 37.

61 Autorité de la Concurrence and Bundeskartellamt (2016), Competition Law and Data. Available at: www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publ.

62 Justice News of the US Department of Justice, Office of Public Affairs, "Former E-Commerce Executive Charged with Price Fixing in the Antitrust Division's First Online Marketplace Prosecution." Available at: www.justice.gov/opa/pr/former-e-commerce-executive-charged-price-fixing-antitrust-divisions-first-online-marketplace.

63 Heather Vogell, "Company That Makes Rent-Setting Software for Apartments Accused of Collusion, Lawsuit Says," ProPublica, 21 Oct. 2022. Available at: https://www.propublica.org/article/realpage-accused-of-collusion-in-new-lawsuit.

64 Heather Vogell, "Pressure Grows on Real Estate Tech Company Accused of Colluding With Landlords to Jack Up Apartment Rents," ProPublica, 14 Nov. 2022. Available at: https://www.propublica.org/article/yieldstar-rent-increase-realpage-lawmakers-collusion.

In these cases, government officials' ability to identify whether an algorithm is designed to facilitate collusion would be key to investigate a pattern when suspicions arise, but absent a review of the underlying code along with datasets and accompanying business documentation, the evidence is not sufficient to prove an anticompetitive conduct.[65]

An often-disregarded goal of the pervasive practice of digital firms' commercial surveillance is engaging in price discrimination, which is the technical term for what Professor Yossi Sheffi of the Massachusetts Institute of Technology (MIT) has called *"the science of squeezing every possible dollar from customers."*[66] Pricing algorithms are a key enabler of this practice. For instance, in 2012, *the Wall Street Journal* reported how Staples' online sales algorithm used customers' location data to charge different prices for the same goods. The algorithm considered the customer's distance from Staples' rivals, such as Office Depot or OfficeMax stores. If rival stores were found within 20 miles, the algorithm automatically offered a discounted price.[67]

Similarly, on-the-job data collection and algorithmic decision-making systems have allowed the use of granular data to produce unpredictable, variable, and personalized hourly pay, a practice dubbed by law professor Veena Dubal as "algorithmic wage discrimination." The clearest example of this practice is currently found in the ridesharing industry, where Dubal found that work allocation systems, dynamic pricing and incentives allow firms like Uber to personalize and differentiate wages for workers in ways unknown to them, paying them as little as the system determines that they may be willing to accept.[68]

AI also enables Big Tech platforms' anti-competitive self-preferencing. In 2017, the European Commission sanctioned Google because its algorithm promoted its own comparison shopper service, called Google Shopping, over competitors, abusing its dominant position in the internet search market. The European authorities found that Google included a number of criteria in its generic search algorithms that resulted in rival comparison shopping services being demoted.[69] The European Commission also preliminarily concluded that Amazon's algorithmic rules and criteria for its Buy Box feature and Prime program unduly favor its own retail business, as well as marketplace sellers that use Amazon's logistics and delivery services.[70]

---

65 Ezrachi & Stucke, op cit. P. 53.

66 James Surowiecki, "In Praise of Efficient Price Gouging," MIT Technology Review, 18 Aug. 2014. Available at: https://www.technologyreview.com/2014/08/19/74207/in-praise-of-efficient-price-gouging/.

67 Jennifer Valentino-DeVries, Jeremy Singer-Vine, and Ashkan Soltani, "Websites Vary Prices, Deals Based on Users' Information," The Wall Street Journal, 24 Dec. 2012. Available at: https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

68 Veena Dubal, "On Algorithmic Wage Discrimination," UC San Francisco Research Paper. 19 Jan. 2023. Available at SSRN: https://ssrn.com/abstract=4331080 or http://dx.doi.org/10.2139/ssrn.4331080.

69 European Commission, 'Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service,' 17 June 2017. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784.

70 European Commission, ;Antitrust: Commission accepts commitments by Amazon barring it from using marketplace seller data, and ensuring equal access to Buy Box and Prime,' 20 Dec. 2022. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777.

Proof of such conduct often is buried in algorithms' code. Even before the European Commission imposed its 2017 sanctions against Google, legal scholars were positing that "*[a]gencies ought to be able to "look under the hood" of highly advanced technologies like the algorithms at the heart of the Google search engine and the data they process.*"[71]

Additionally, agencies might need to require disclosure of algorithmic information to protect competition in regulated industries. For instance, until 2004, the U.S. Department of Transportation required companies operating computer reservation systems (CRS) for air travel to share the ranking criteria used in sorting algorithms for displayed flights, including "*the specifications used by the system's programmers in constructing the algorithm.*"[72]

The source code and algorithmic secrecy guarantees that tech interests are pushing for to be included in "digital trade" deals are likely to get in the way of agencies or private parties being able to "look under the hood."

The narrow exceptions supported by tech interests could limit antitrust enforcers' ability to effectively fight anticompetitive behavior.

Plus, industry-wide requirements to disclose algorithmic information about ranking criteria and system specifications, such as those applied by the Department of Transportation to CRS until 2004, would certainly not be covered by USMCA's narrow exception.

For instance, the USMCA exception to its source code and algorithm secrecy provision only permits source code disclosure requests or orders by regulatory bodies or judicial authorities and only "*to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding.*" (emphasis added). Namely, the exception only applies after a government agency or private party has sufficient evidence of a violation of a law or right to meet a burden of proof to be able to obtain more information, whether through an agency investigation, court order, or civil suit discovery. (Note that the exception allows disclosure "*to the regulatory body*", meaning that it is unclear whether a private party filing a lawsuit could be allowed to gain access to the required information under this rule.) Yet it may well not be possible to meet that burden of proof without having access to the information about the source code or algorithm, along with the dataset and relevant business documentation, that reveals the antitrust or other violation. And even for agencies whose statutes provide broad investigatory authority, the limitation for "specific" investigation calls into question whether such trade-pact language would encompass a broad investigation into an economic sector or general practices of a firm rather than for a specific suspected violation. Plus, industry-wide requirements to disclose algorithmic information about ranking criteria and system specifications, such as those applied by the Department of Transportation to CRS until 2004, would certainly not be covered by USMCA's narrow exception.

71 Frank Pasquale, The Black Box Society: the secret algorithms that control money and information, Harvard University Press, 2015.

72 14 CFR 255.4 (3); Upturn and Omidyar Network, Public Scrutiny of Automated Decisions: Early Lessons and Emerging Methods. Available at: https://omidyar.com/wp-content/uploads/2020/09/Public-Scrutiny-of-Automated-Decisions.pdf.

The EU model for this exception is equally problematic as it covers source code disclosures required to "*remedy a violation of competition law*."[73] This leaves out the disclosures required to unveil or prove that such a violation has indeed occurred.

Conclusion

Corporate interests are advocating for strict limits on government access to source code and even detailed information about algorithms that would effectively establish extreme source code and algorithm secrecy guarantees in U.S. "trade" agreements.[74] Obviously, such terms have nothing to do with trade, but rather represent an effort by special interests to use closed-door international negotiations on future international agreements to lock in powers and rights for themselves that would be difficult to achieve through public debate in more open policymaking venues.

These provisions are premised on the notion that private commercial interests prevail over the public interest. This briefing paper shows how algorithmic transparency and accountability is essential to ensure that AI works in favor of the public and not against it. Yet, if trade deals impose limits on the capacity of governments and courts to mandate disclosure of source code and other algorithm-related information, tech companies could eviscerate prospective regulation and evade government oversight.

It is notable that only 11 of the 181 agreements with ecommerce or digital trade provisions negotiated since 2000 include obligations to limit government access to source code,[75] showing how controversial this particular concept is.

In addition to the fact that "digital trade" source code secrecy provisions are at odds with algorithmic transparency and accountability principles, there is no rationale that justifies granting these special interests extraordinary new privileges and rights. Tech firms that wish to protect their proprietary source code and algorithms can rely on existing intellectual property and trade secrets protections. If a company develops pathbreaking software, it can copyright the code and/or request patent protection to secure the right to commercialize and use the software exclusively, including its source code, with certain exceptions. If the same company does not want to register a copyright or file for a patent, as long as the algorithm complies with the requirements enshrined in existing regulation, it can rely on existing protections to undisclosed information to ensure its code is not improperly accessed or shared.[76]

---

73 See Article 8.73.2(a) of the EU-Japan Economic Partnership Agreement.

74 The U.S. Chamber of Commerce has announced in its "digital trade priorities" that it wants rules that would guarantee that "companies should not be forced to transfer their technology—including source code and proprietary algorithms—to competitors or governments." This is code for the type of source code provisions that would prevent governments from demanding access to source on behalf of the public interest. See U.S. Chamber of Commerce, "The Digital Trade Revolution," P. 19. Available at: https://www.uschamber.com/assets/documents/Final-The-Digital-Trade-Revolution-February-2022_2022-02-09-202447_wovt.pdf.

75 Calculations made using the TAPED dataset under the project 'The Governance of Big Data in Trade Agreements,' Universities of Lucerne and Bern. Accessed on 3 Oct. 2022. Available at: https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/research/taped/.

76 Ulla-Maija Mylly, "Preserving the Public Domain: Limits on Overlapping Copyright and Trade Secret Protection of Software,". IIC 52, 1314–1337 (2021). Available at: https://doi.org/10.1007/s40319-021-01120-3; International Trade Union Confederation, op cit. P. 4.

These existing protections already are required by the World Trade Organization's Agreement on Trade-Related Aspects of Intellectual Property, applicable to the entire WTO membership, which encompasses over 95% of the world economy.[77]

Industry's "digital trade" agenda would excavate the policy space out from under Congress and various U.S. agencies before governments can act while also undermining policies already enacted or being developed all over the world. The challenges and opportunities accompanying the growth of the digital economy have generated congressional and agency action aimed at protecting the public from online harms and ensuring that the benefits of the digital economy are widely distributed. The U.S. government is behind other countries in launching such initiatives. Tech interests are trying to derail algorithmic accountability efforts and other elements of the digital governance push. As governments sort out their own policies, it will be helpful to enhance cooperation between countries to deal with the key issues that these technologies pose. One thing that should not be on any agenda, much less slipped into trade agreements under the brand of "digital trade," are handcuffs on legislators, regulators, and courts as they tackle these challenges.

77 "Member states of the WTO: World Trade Organization," WorldData. Accessed 9 May 2022. Available at: https://www.worlddata.info/alliances/wto-world-trade-organization.php

The American Economic Liberties Project is a new, independent organization fighting against concentrated corporate power to realize economic liberty for all, in support of a secure, inclusive democratic society.

Rethink Trade was established to intensify analysis and advocacy regarding the myriad ways that today's trade agreements and policies must be altered to undo decades of corporate capture and to deliver on broad national interests.

economicliberties.us
@econliberties
info@economicliberties.us

rethinktrade.org
@rethinktrade
info@rethinktrade.org

“Digital Trade” Doublespeak: Big Tech’s Hijack of Trade Lingo to Attack Anti-Monopoly and Competition Policies

November 2022

Daniel Rangel
Taylor Buck
Erik Peinert
Lori Wallach

About the Authors

Daniel Rangel is the Research Director of the Rethink Trade program at the American Economic Liberties Project. A lawyer, Daniel specializes in international trade and investment law and policy. He is an expert in trade and labor matters and is one of the few lawyers actively filing stakeholder petitions to activate the USMCA Rapid Response Mechanism.

Taylor Buck is the Program Associate at the Rethink Trade program at the American Economic Liberties Project and is a recent graduate of the University of North Carolina at Chapel Hill.

Erik Peinert manages and coordinates the American Economic Liberties Project's policy and research agenda. A political scientist specializing in economic policymaking, competition and market power, he is authoring a book on the evolution of antitrust and monopoly in the 20th century. Erik is also an affiliated researcher at the Rhodes Center for International Finance at Brown University.

Lori Wallach is the director of the Rethink Trade program at the American Economic Liberties Project and a 30-year veteran of international and U.S. congressional trade debates. A lawyer, Lori is the author of *The Rise and Fall of Fast Track Trade Authority and Whose TradeOrganization? A Comprehensive Guide to the WTO*.

Introduction

As digital mega-platforms have continued to grow in size and expand their influence over every aspect of peoples' public and private lives, U.S. policymakers and those worldwide have begun wrestling with thorny questions of digital governance. Regulatory efforts span from data privacy and security to artificial intelligence transparency and accountability to labor rights for gig workers, but there is one area where Big Tech is fighting tooth and nail: policies targeting their monopoly power and promoting fair competition. Predatory behavior and lax antitrust enforcement,[1] along with network effects and "winner-takes-all" dynamics in digital markets,[2] have led to monopolies in the digital services that the vast majority of people use daily.

After years of abuses, and advocacy from smaller businesses, consumers, and workers in response, policymakers worldwide have begun introducing policies to rein in Big Tech's dominance over the digital economy. Some of the most common measures aim at increasing competition by establishing strict rules for app store operators' duopoly; forbidding certain anticompetitive practices from digital "gatekeepers;" addressing the power imbalance between media outlets and the mega-platforms that currently determine what kind of content ends up reaching the public; and stopping anticompetitive behavior before it happens.

Big Tech is employing all tactics to fight against these efforts. Digital firms have deployed thousands of lobbyists to sway legislators and regulators. Industry groups and the organizations and academics they fund circulate throughout every major policy center repeating Big Tech's talking points against new regulations. Executives and former lobbyists of these companies cycle back and forth between these firms and government positions, using the revolving door to try to maintain lax privacy standards, to attack antimonopoly initiatives in other countries, and to counter limitations on data mobility through international negotiations.[3]

However, an under-the-radar strategy has also emerged. Big Tech has begun to co-opt trade negotiating venues worldwide and hijack international trade law jargon to use trade enforcement mechanisms to attack other countries' policies that constrain digital platforms' monopolistic size and anticompetitive behavior.

1 Matt Stoller, Sarah Miller and Zephyr Teachout, "Addressing Facebook and Google's Harms Through a Regulated Competition Approach," American Economic Liberties Project. April 10, 2020. Available at: https://www.economicliberties.us/our-work/addressing-facebook-and-googles-harms-through-a-regulated-competition-approach/; Matt Stoller, Pat Garofalo and Olivia Webb, "Understanding Amazon: Making the 21st-Century Gatekeeper Safe for Democracy," American Economic Liberties Project. July 24, 2020. Available at: https://www.economicliberties.us/our-work/understanding-amazon-making-the-21st-century-gatekeeper-safe-for-democracy/.

2 Mariana Mazzucato, "Preventing Digital Feudalism," Project Syndicate. Oct. 2, 2019. Available at: https://www.project-syndicate.org/commentary/platform-economy-digital-feudalism-by-mariana-mazzucato-2019-10. The House Antitrust Report on Big Tech, Oct. 6, 2020. Available at: https://www.nytimes.com/interactive/2020/10/06/technology/house-antitrust-report-big-tech.html.

3 Mekedas Belayneh, "Big Tech's Back Door to Digital Trade Rules," The American Prospect. June 14, 2022. Available at: https://prospect.org/power/big-techs-back-door-to-digital-trade-rules-commerce-gina-raimondo/.

When deployed in the context of ongoing trade negotiations, this strategy is also aimed at preventing regulation in the United States by locking in binding constraints on domestic policy within the rules of international trade pacts. Simultaneously, Big Tech is seeking to harness U.S. domestic trade enforcement tools to try to roll back or chill establishment of strong policies in other countries. Getting such policies in other nations labeled as illegal trade barriers would also undermine the domestic push for greater regulation in the United States. This ploy only stands a chance to be effective because of its distracting "trade" camouflage.

The inception of so-called "digital trade" rules in international agreements is still in an early stage, particularly at the multilateral level, yet such terms already have been included in agreements signed by the United States and some other countries.[4] One of the terms pushed by Big Tech in trade-pact negotiating venues is based on hijacking a bedrock trade concept known as "non-discrimination."

Non-discrimination is as old as the first trade agreements and, in its most basic form, requires countries to treat products the same regardless of their national origin. When applied to trade in goods, that means a country must provide an imported good with the same treatment it gives to its own producers' "like" goods and also not treat the imported goods from one country differently than from another country. For instance, if a country requires driver and passenger dashboard airbags in domestic automobiles, it can do the same for imported cars, but cannot only require that imported cars also have side impact airbags, or that imports from Japan get the domestic standard but imports from Korea get a tougher one. The idea was that "like goods" should be allowed to compete on equal terms regardless of where they were made. Thus, initially, the non-discrimination standard especially targeted facially discriminatory policies – or those that clearly had a discriminatory intent. However, as trade-pact rules expanded into setting policies that apply to the service sector and other areas of regulation that had previously been the sole bailiwick of domestic policy, commercial interests pushed to expand the

non-discrimination standard. Most trade agreements signed since the 1990s include language that can be used to attack origin-neutral policies that may have a disproportionate *effect* on a set of products of foreign origin. And even before trade pacts included broader language, trade-pact enforcement panels contributed to the perilous expansion of the non-discrimination standard by judging facially neutral policies with inadvertent differential impacts as illegal trade barriers.[5]

Big Tech is trying to take advantage of those extensive interpretations and rules to establish new grounds to attack policies around the world that attempt to regulate

4 See International Trade Union Confederation, E-Commerce Free Trade Agreements, Digital Chapters and the Impact on Labour. (London, 2019). Available at: https://www.ituc-csi.org/IMG/pdf/digital_chapters_and_the_impact_on_labour_en.pdf.

5 For instance, in 1992, a panel under the General Agreement on Tariffs and Trade (GATT) determined that certain tax benefits provided to microbreweries in the United States were inconsistent with GATT Article III (national treatment) because larger Canadian beer producers could not access them. U.S. large breweries were also ineligible. See: Panel Report, United States – Measures Affecting Alcoholic and Malt Beverages, DS23/R, adopted 19 June 1992, BISD 39S/206. Available at: https://worldtradelaw.net/document.php?id=reports/gattpanels/usmaltbeverages.pdf.

the most dominant digital corporations. "Non-discrimination" provisions in existing "digital trade" deals[6] and in a proposed World Trade Organization-adjacent multilateral "e-commerce" agreement[7] forbid domestic digital policies that may have a discriminatory effect. That lingo captures neutral policies that may have a larger impact on the largest firms simply because they are large. That is to say, even when the predominant underlying motive of a policy is not related to the place from which digital services are provided or the country of incorporation of said firms, a neutral domestic policy may have greater effect on firms that dominate a market. For example, consider a domestic policy that requires *all domestic and foreign* online ride-hailing services to register as taxi companies and meet policies applicable to other such firms. This neutral policy would not be considered discriminatory on its face, but it would have a greater effect on, say, Uber, if Uber had the largest share of a country's online ride-hailing services.

This report documents the way in which Big Tech has used trade lingo to claim "discriminatory" treatment and seek enforcement and penalties against governments that have adopted or have even discussed the implementation of competition policies that may have a larger impact on dominant digital firms due to their size and role in the market – not their nationality. Since the Big Tech firms have not yet achieved their goal of deploying corporate-led "digital trade" deals worldwide, today these firms are using the somewhat less intrusive e-commerce chapters negotiated by the United States in the 2000s – when the digital economy was merely awakening – and also seeking to employ domestic trade enforcement tools for their attacks.

A favored vehicle for this approach has been the U.S. National Trade Estimate (NTE) report. The NTE is a statutorily required annual review of what ostensibly are trade-partner countries' illegal trade barriers that is issued by the Office of the United States Trade Representative (USTR). The NTE, which is based in part on policies brought to USTR's attention through a request for private sector input, has been used by corporations as a hit list. For years, the NTE has been used to attack as trade barriers other countries' public interest policies that various industries dislike. The NTE is, effectively, a government-sponsored corporate hit list arming industry interests to attack similar policies domestically. The Internet Tax Freedom Act added "barriers to United States electronic commerce" to the list of policies under the purview of the NTE in 1998. This opened the door for Big Tech interests to demand that U.S. government officials elevate their private peeves against digital governance policies adopted by other nations into official U.S. trade policy.

6 See, for instance, Article 19.4 of the United States-Mexico-Canada Agreement: "Non-Discriminatory Treatment of Digital Products: No Party shall accord less favorable treatment to a digital product created, produced, published, contracted for, commissioned, or first made available on commercial terms in the territory of another Party, or to a digital product of which the author, performer, producer, developer, or owner is a person of another Party, than it accords to other like digital products." .

7 WTO Electronic Commerce Negotiations Consolidated Negotiating Text, Sep. 2021. Available at: https://www.bilaterals.org/IMG/pdf/wto_plurilateral_ecommerce_draft_consolidated_text_september_2021.pdf

The way in which digital firms and their trade associations have tried to weaponize this review to attack pro-competition policies and label them as "discriminatory" or "barriers to digital trade" provides a preview of what they could do if Big-Tech-rigged "digital trade" rules are expanded in bilateral, regional, and multilateral trade agreements. Particularly dangerous would be the inclusion of broad, open-ended non-discrimination clauses in these deals. In order to carry out this analysis, we identified four pioneering policies around the world that are revolutionizing digital governance from a competition policy perspective:

i. Korea's promotion of increased competition in the app market by requiring that app stores allow diverse payment systems (not only their own) and do not forbid app developers from selling on other platforms (Korea's App Stores Law);

ii. Australia's remedy for Big Tech platforms' monopolization of ad revenue and resulting decimation of local journalism by creating the conditions necessary for digital platforms to pay for the news they distribute (Australia's News Media Bargaining Code);

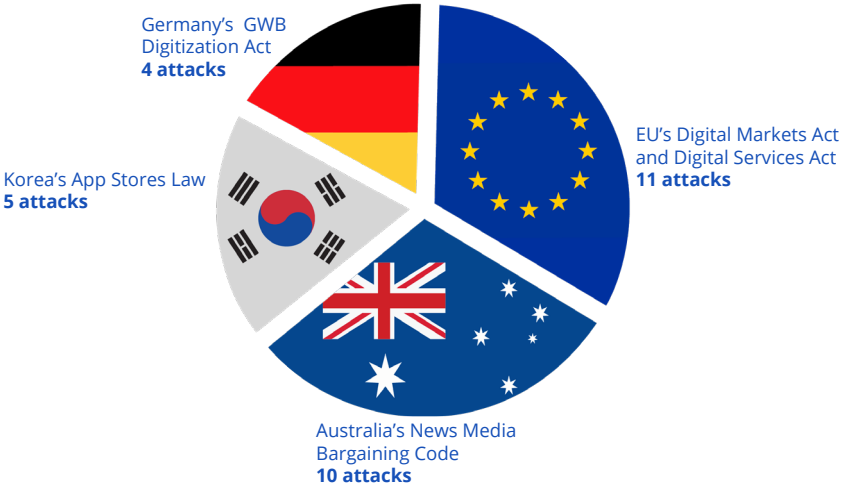
iii. the European Union's crackdown against abusive behavior by dominant digital firms and establishment of consumer rights online (EU's Digital Markets Act and Digital Services Act);

iv. Germany's competition law revamp that proactively prevents anticompetitive actions by the biggest digital players (Germany's GWB Digitization Act).

Countries around the world are considering adoption of similar policies, including the United States. As forerunners in the global effort to rein in Big Tech, each of these policy initiatives have come under fierce attack by the digital mega-platforms, including myriad attacks using the NTE process. The report identifies 30 NTE industry comments that used trade jargon to criticize cutting-edge competition policies. A complete list of these submissions can be found in the annex to this report.

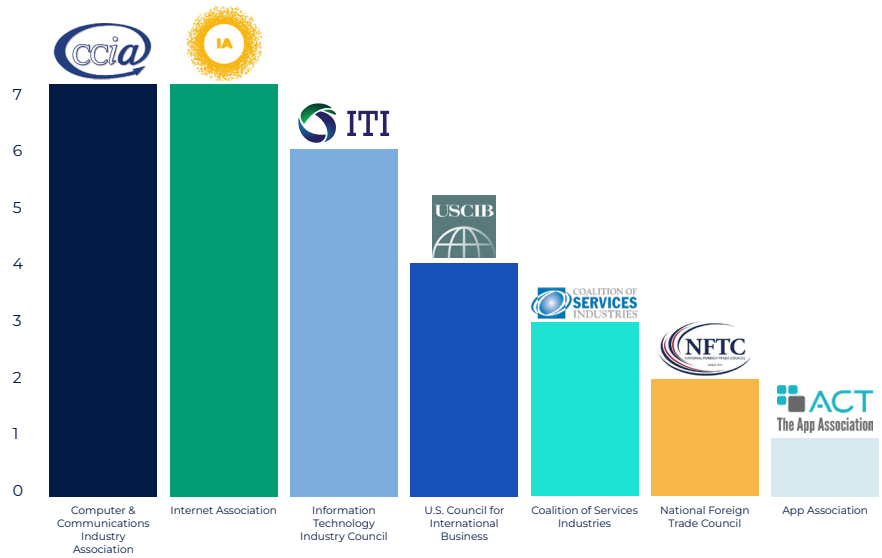
The policies that received more attacks were the EU's Digital Markets Act and Digital Services Act with 11 comments, followed by Australia's News Media Bargaining Code with 10 comments, Korea's App Stores Law with five comments, and Germany's GWB Digitization Act with four comments. This indicates that Big Tech interests are consolidating their well-coordinated attacks on the most expansive policies revolutionizing antitrust law to protect their free ability to crush competitors and abuse smaller companies.

Number of NTE Attacks Against Global Digital Competition Policies



As for the organizations, the Computer & Communications Industry Association and the now-defunct Internet Association were the groups that most often used trade lingo to attack competition policies adopted by other nations. These associations both include Amazon, Google, Microsoft, and other Big Tech companies among their membership. Other organizations that routinely used their NTE submissions to challenge the analyzed policies using trade "non-discrimination" language are the Information Technology Industry Council, the U.S. Council for International Business, the Coalition of Services Industries, the National Foreign Trade Council, and the App Association.

Number of NTE Attacks Against Digital Competition Policies by Organization



To construct a thorough inventory of those attacks, we reviewed each industry submission for the 2021 and 2022 versions of the NTE reports – hence, submissions filed in 2020 and 2021 – and analyzed how they impacted the U.S. government positioning vis-à-vis the targeted policies. We also explain how the U.S. Congress is currently discussing several bills that mirror some of the most important elements of the analyzed policies. In both years, industry submissions assailed each of the four policies as "discriminatory" and attempted to recruit the U.S. government to join Big Tech's crusade against them. As the Biden administration develops its own digital governance strategy and after it adopted an all-government anti-monopoly policy, thankfully the U.S. government attitude has shifted. While, the current administration has not adopted the industry line without question, the industry submissions show the perils of extending a network of "digital trade" agreements that can worsen the obstacles to creating a fair and competitive digital economy.

South Korea's Global-First Move to Foster Fair App Stores Attacked by Google and Apple

For years, digital items purchased within apps – like extra lives in Candy Crush, or a premium subscription to remove ads in Spotify – have offered Big Tech giants like Apple and Google a lucrative – and exclusive – hidden market to monopolize to the detriment of app creators and purchasers alike. When users buy digital goods in an app on Apple's iOS or Google's Android, Apple and Google require that their payment systems be used to process the purchase. Forcing developers and consumers to use their systems allows Apple and Google to charge a sales commission fee of up to 30%, generating massive revenues for these two dominant firms. As the sole major players in the app store market, Apple and Google have the power to dictate terms for developers and impose fees as they please.

In August 2021, South Korea became the first country in the world to try to crack open this market. An amendment to Korea's Telecommunications Business Act bans companies that operate app stores and enjoy a dominant position in the market, like Apple and Google, from forcing app developers to use the firms' own payment systems. Instead, companies now have to allow users the option to pay for in-app purchases with various third-party payment systems.[8]

The legislation emerged in 2020 after Google announced that all apps on the Google Play store would have to use the company's own payment system – i.e., pay the 30% commission. Previously, that requirement applied only to gaming apps.

8 "South Korea: Amended Telecommunications Business Act Will Ban App Payment Monopolies," Library of Congress, 2021. Available at: https://www.loc.gov/item/global-legal-monitor/2021-09-16/south-korea-amended-telecommunications-business-act-will-ban-app-payment-monopolies/

The new Korean policy protects both consumers and developers from Big Tech companies abusing their dominant market positions by forcing services on them and setting unfair prices. Violations of the amendment can result in fines up to 2% of a company's South Korean revenue.

Notably, the Korean law that was enacted to end anticompetitive app store practices is similar to U.S. House and Senate proposals that currently enjoy broad bipartisan support. Particularly, the Senate version, the Open App Markets Act, was approved by the Judiciary Committee on February 3, 2021.[9] Senior Republican members of Congress have app store legislation as a top legislative priority,[10] showing that the enactment of U.S. legislation similar to the Korean law is a real possibility and not only a Democratic Party goal.

The Korean law and American proposal also fall well within traditional antitrust prohibitions against "tying." This is an anti-competitive practice by which a company makes the sale of one product or service conditional upon also purchasing a separate product or service. Google is in fact currently facing an antitrust lawsuit in the United States alleging that its tying of Google Play Billing to its app store is an illegal violation of the Sherman Antitrust Act.[11] These app store laws simply seek to enhance the clarity and enforcement mechanisms for such rules.

Despite this, Apple and Google pushed U.S. trade officials to attack the Korean legislation as "discriminatory" while it was being considered by South Korea's parliament. They argued that it would affect them more than other businesses.[12] They claimed the Korean law was an attack against U.S. businesses, conveniently avoiding the reality that the law would impact them more because of their monopoly practices. The two firms mobilized supposedly regional organizations to hint at the potential of sparking a trade dispute. In July 2021, the Asia Internet Coalition, a group backed by Apple and Google in spite its seemingly international name, stated that the law "*could provoke trade tensions between the United States and South Korea.*"[13]

Apple and Google used the NTE process as one of the main vehicles to push their grievances and attempt to recruit the U.S. government in their fight against the Korean legislation. The Information Technology Industry Council (ITIC), a D.C.-based trade association that includes Apple and Google as members, urged the U.S. government to weigh in against the Korean policy in a public submission to USTR in October 2020. The ITIC claimed that the "*legislative intent*" of the amendment was "*to target US firms, while*

9 Lauren Feiner, "Senate Committee advances bill targeting Google and Apple's app store profitability," CNBC, Feb. 3, 2022. Available at: https://www.cnbc.com/2022/02/03/senate-committee-advances-open-app-markets-act.html

10 John Hendel, "Tech antitrust optimism to kick off April," POLITICO, Apr. 1, 2022. Available at: https://www.politico.com/newsletters/morning-tech/2022/04/01/tech-antitrust-optimism-to-kick-off-april-00022252. David O. Williams, "Ken Buck Battles Big Tech With Bill to Unlock App Stores' Rules," Colorado Times Reporter, Sept. 24, 2021. Available at: https://coloradotimesrecorder.com/2021/09/ken-buck-battles-big-tech-with-bill-to-unlock-app-store-rules/39899/

11 See Second Amended Complaint, In Re Google Play Developer Antitrust Litigation, Case No. 3:20-cv-05792-JD (Filed 01/24/22, N.D. Cal.). Available at: https://www.docketalarm.com/cases/California_Northern_District_Court/3--21-md-02981/In_re--_Google_Play_Store_Antitrust_Litigation/182/

12 David McCabe and Jin Yu Young, "Apple and Google's Fight in Seoul Tests Biden in Washington," The New York Times, Aug. 23, 2021. Available at: https://www.nytimes.com/2021/08/23/technology/apple-google-south-korea-app-store.html?searchResultPosition=10

13 Ibid

favoring their Korean competitors," and also argued that the policy would be a violation of market access and investment commitments under the Korea-U.S. Free Trade Agreement (KORUS).[14]

The 2021 NTE report, largely drafted before the current USTR took office, echoed Apple and Google's allegations, stating that the legislation *"appears to specifically target U.S. providers and threatens a standard U.S. business model that has allowed successful Korean content developers to reach global audiences."* [15]

By the time comments for the next NTE report were due, industry interests had closed ranks: Four trade associations backed by Apple and Google attacked the amendment in remarkably similar language. These associations claimed that the amendment violated commitments under KORUS by targeting U.S. companies to benefit Korean competitors. Notably, the Coalition of Services Industries and the Internet Association used the exact same language that the 2021 NTE report included to criticize this initiative, the recycled the language is: the Korean App Store Law *"threatens a standard US business model that has allowed successful Korean content developers to reach global audiences."* [16]

Other NTE Industry Attacks on the South Korean App Store Legislation

- Information Technology Industry Council (October 2021): **"The [App Stores] law appears to run contrary to Korean trade commitments** by taking an approach that would disrupt standardized practices that ensure consumer privacy, security, and reliable access across markets, and with **legislators' public statements effectively singling out two U.S.-headquartered companies**. The law will also restrict U.S. app developers' ability to reach the Korean market via trusted ecosystems." (emphasis added).
- Coalition of Services Industries (October 2021): "**This legislation is global-first and bans a business model that is practiced by US mobile app marketplace providers, and not their Korean equivalents**. It threatens a standard US business model that has allowed successful Korean content developers to reach global audiences, and **is at tension with Korea's obligations under the Korea-US FTA.**" (emphasis added).
- Computer & Communications Industry Association (October 2021): "**The scope of the law effectively creates a band on a predominately used U.S. model, at the exclusion of local equivalents**. Further, policymakers supportive of the bill have made clear their intent to single out specific U.S. companies with the new law. **The targeting of U.S. firms could conflict with Korea's trade commitments under the Korea-U.S. Free Trade Agreement, as well as commitments under Article XVII (National Treatment) of the WTO General Agreement on Trade in Services (GATS)**." (emphasis added).
- Internet Association (October 2021): "**This legislation is a global-first move that affected only two U.S. digital companies and none of their Korean competitors**. It threatens a U.S. business model that has allowed successful Korean content developers to reach global audiences, and **is at tension with Korea's obligations under the Korea-U.S. FTA.**" (emphasis added).

14 ITI Response to USTR Request for Public Comments to Compile the National Trade Estimate Report (NTE) on Foreign Trade Barriers. P. 48. Oct. 29, 2020. Available at: https://www.itic.org/policy/ITI2021NTEPublicCommentFinal.pdf

15 2021 National Trade Estimate Report on Foreign Trade Barriers, page 333. Available at: https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf

16 2021 Coalition of Services Industries (CSI) Submission: Comments for the National Trade Estimate Report on Foreign Trade Barriers Docket Number USTR-2021-0016. P. 47. Available at: https://www.regulations.gov/comment/USTR-2021-0016-0057; Internet Association Submission For The 2022 USTR National Trade Estimate Report Docket No. USTR-2021-0016. P. 83. Available at: https://www.regulations.gov/comment/USTR-2020-0034-0028.

In the 2022 NTE report, the Korean app store policy was still listed as a barrier to digital trade and electronic commerce, although this time USTR refrained from elevating Big Tech's incriminating language against the new South Korean law and did not opine on it, nor did it suggest that the new legislation was discriminatory or that it targeted U.S. providers.[17]

Though Apple and Google agreed to comply with the law after it came into effect in September 2021, both were slow to follow through.[18] Google seems to have failed to comply with the new policy and instead continued to charge commissions to app developers, even when users opted for third-party payment systems. In April 2022, the Korea Communications Commission began a provisional investigation currently ongoing to determine if any app market operators were in violation of the policy.[19] In June, Apple announced app developers in Korea only will be allowed to use third-party service providers. But the concession comes with a series of restrictions: Alternative providers will have to apply and be pre-approved by Apple, and the company will continue to take a 26% commission for any purchases made through such providers. This means that for a third-party payment intermediary to be competitive, it would have to charge less than 4% of the transaction value.[20] In August, the Communications Commission began a formal investigation to determine if Apple, Google, and a domestic app store operator called One Store are not complying with the with the new law.[21]

These latest developments show Apple and Google's intent to continue and fight against the policy, and new trade-based attacks might arise. Additionally, the inclusion of a domestic company in the probe discredits the discrimination claims launched by U.S. Big Tech firms.

17 [17] 2022 National Trade Estimate Report on Foreign Trade Barriers, page 326. Available at: https://ustr.gov/sites/default/files/2022%20National%20Trade%20Estimate%20Report%20on%20Foreign%20Trade%20Barriers.pdf

18 Joyce Lee, "S. Korea lawmaker says Apple, Google not doing enough to comply with app store law," Reuters, Nov. 16, 2021. https://www.reuters.com/technology/skorea-lawmaker-says-apple-google-not-doing-enough-comply-with-app-store-law-2021-11-16/

19 Simon Sharwood, "Google snubs South Korea's app store law," The Register, Apr. 6, 2022. Available at: https://www.theregister.com/2022/04/06/google_south_korea_app_payments_illegal/. Mariella Moon, "Korean authorities tell Google it can't remove apps that link to external payment," Yahoo!Finance, Apr. 6, 2022. Available at: https://finance.yahoo.com/news/korea-kcc-app-store-law-google-external-payments-114054384.html. See also "Korea regulator to examine app payment practices of Google, Apple, One Store," Telecompaper, May 19, 2022. Available at: https://www.telecompaper.com/news/korea-regulator-to-examine-app-payment-practices-of-google-apple-one-store--1424948.

20 Jon Porter, "Apple lets apps in South Korea use third-party payment systems," The Verge, Jun. 30, 2022. Available at: https://www.theverge.com/2022/6/30/23189384/apple-south-korean-app-store-third-party-payment-systems-in-app

21 Laura Dobberstein, "South Korean regulator worried Apple, Google, may be working around app store payment choice law," The Register, Aug. 10, 2022. Available at: https://www.theregister.com/2022/08/10/apple_google_south_korea_investigation/

Australia's Strategy to Level the Playing Field in News Media Advertising and Big Tech's Staunch Opposition

When journalists publish new stories, nowadays they rely on digital platforms like Facebook and Google to help their content reach users. Facebook and Google in turn rely on news media content to generate revenue through user engagement. It's an interdependent relationship, but one with a serious power imbalance: Media businesses need their content on the major digital platforms to reach the public, but the digital platforms don't need any one news business' content to entice users. This asymmetry means that although news content generates massive revenue for digital platforms, journalists and publishers don't receive a cut to continue funding their journalism.

Australia set out to address this imbalance with a mandatory code of conduct. It allows eligible news businesses to bargain individually or collectively with designated digital platforms, which could include Facebook and Google, to be paid when the platforms link to the news businesses' content on platform news feeds or in search results. The new policy passed the Australian parliament in February 2021. By ensuring news businesses are fairly paid for their content, the code aims to sustain local public interest journalism.

The code has four components.[22] First, designated digital platform companies must bargain in good faith with registered news business corporations. To be registered, news businesses must apply to the Australian Communications and Media Authority and meet a series of eligibility criteria. Designation of digital platforms is done by the Australian Treasurer, who must consider whether there is a significant bargaining power imbalance between the platform and news media businesses. Second, compulsory arbitration rules come into effect when bargaining parties are unable to negotiate an agreement. In these instances, both the digital platform and the news business present a final take-it-or-leave-it offer, an arbitral panel makes a final decision between the two.

The compulsory arbitration rules put the digital platforms and the news media businesses on more even footing: Neither party wants to risk the arbitral panel choosing the others' final offer, so it is in their best interest to come to an agreement without triggering the compulsory arbitration rules. The third component of the code dictates how platforms deal with the news content they host. Under these requirements, digital platforms are required to give news businesses a 14-day notice of any planned algorithmic changes or internal practices likely to have a significant effect on referral traffic to their content.

22 See News Media and Digital Platforms Mandatory Bargaining Code Act of 2021. Available at: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6652.

Digital platforms must also provide news businesses with clear explanations of the types of data collected by the digital platform as users interact with news content. Finally, non-differentiation requirements prevent digital platforms from treating registered news businesses differently from unregistered news businesses in terms of making news content available.

The Australian law is similar to the Journalism Competition and Preservation Act (JCPA), which is currently under consideration in the United States.[23] The JCPA, like the Australian law, creates a temporary antitrust "safe harbor" for certain publishers (smaller ones) to organize and collectively negotiate with large digital platforms in order to address the major disparity in bargaining power between news publishers – who have been struggling with bankruptcy – and platforms. Like the Australian law, the JCPA also outlines a framework for collective negotiations between publishers and platforms. The Senate Judiciary Committee voted in favor of the JCPA in September 2022 and sent the bill toward floor consideration by the full Senate.[24]

The push for the legislation in Australia began in 2017, when the Australian Competition and Consumer Commission (ACCC) was directed to consider the impact of online search engines, social media, and digital content aggregators on competition in the media. The subsequent 2019 Digital Platform Inquiry found an imbalance in bargaining power between digital platforms and news businesses. The Inquiry concluded that this imbalance excludes news businesses from getting a share of any revenue generated by the content they create when it is posted on digital platforms. According to the Inquiry, Facebook and Google are "unavoidable trading partners" news media rely on for referral services. Therefore, both mega-platforms have substantial bargaining power that influences the ways news outlets conduct business with Facebook and Google.[25]

After the release of the Inquiry, the Australian government directed Google and Facebook to develop voluntary agreements with news media. The government warned that if voluntary agreements could not be met, alternative options, including a mandatory code, would be explored. Attempts to develop a voluntary code were unsuccessful and the ACCC concluded that reaching such an agreement would be "unlikely."[26] Meanwhile,

23 S.2710 – 117th Congress (2021-2022): Open App Markets Act. Available at: https://www.congress.gov/bill/117th-congress/senate-bill/2710.

24 Senate Committee on the Judiciary, 'Judiciary Committee Advances Bipartisan Journalism Competition and Preservation Act,' Sept. 22, 2022. Available at: https://www.judiciary.senate.gov/press/dem/releases/judiciary-committee-advances-bipartisan-journalism-competition-and-preservation-act.

25 Australian Competition and Consumer Commission Digital Platforms Inquiry. Available at: https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.

26 Nour Haydar, "Facebook and Google to face mandatory code of conduct to 'level playing field' with traditional news media," ABC, Apr. 19, 2020. Available at: https://www.abc.net.au/news/2020-04-20/facebook-and-google-to-face-mandatory-code-of-conduct/12163300.

the pandemic led to a surge in visitors to news websites, but advertising revenue sharply dropped as consumers spent less, further stressing the already shrinking media industry and prompting the government to develop a mandatory code.[27]

Big Tech swept in to protest the development of the mandatory code, again using trade lingo in an attempt to block the policy from moving forward.

In a submission to the ACCC, the U.S. Chamber of Commerce claimed that the law would restrict access to digital services in Australian markets and violate both the Australia-U.S. Free Trade Agreement (AUSFTA) and the World Trade Organization's General Agreement in Trade in Services' (GATS) national treatment obligations (i.e., non-discrimination) by exclusively targeting leading U.S. technology companies to help domestic companies. The Chamber of Commerce argued that two American companies, Google and Facebook, were repeatedly being singled out by Australian officials drafting the code and that this was precisely what national treatment obligations were designed to counter.[28] In another submission, the Software and Information Industry Association (SIIA), a D.C.-based trade association that includes Facebook and Google among its members, echoed concerns over discriminatory targeting of U.S. companies in a submission to the Australian Senate. The SIIA also suggested that the code's requirement for digital platforms to provide news media with information regarding planned changes in algorithms was a violation of AUSFTA intellectual property protections and that the lack of options for appeal of regulators' decisions violates AUSFTA's minimum standard of treatment for investors and transparency rules.[29] In another submission, the Information Technology Industry Council likewise argued that the code violated AUSFTA national treatment and most-favored nation rules by targeting American companies.[30] In its own submission, the Internet Association wrote that the code is "fundamentally discriminatory towards U.S. companies, sets a harmful global precedent, and undercuts critical principles of an open internet."[31]

27 Josh Taylor, "Facebook and Google to be forced to share advertising revenue with Australian media companies," The Guardian, Apr. 19, 2020. Available at https://www.theguardian.com/media/2020/apr/19/facebook-and-google-to-be-forced-to-share-advertising-revenue-with-australian-media-companies.

28 US Chamber of Commerce Submission on News Media Bargaining Code, Aug. 27, 2020. Available at: https://www.accc.gov.au/system/files/US%20Chamber%20of%20Commerce.pdf .

29 PDFs of all submissions regarding the code to the Australian Senate Standing Committee on Economics can be viewed at: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/TLABNewsMedia/Submissions.

30 Ibid

31 Internet Association Submission on News Media Bargaining Code, Jan. 15, 2021. Available at: https://www.aph.gov.au/DocumentStore.ashx?id=e73c1237-ef36-4fdc-878e-1db2af19668a&subId=700038.

Other 2020 NTE Industry Attacks on the Australian News Media Code

- **Information Technology Industry Council (October 2020):** "The Code not only requires digital platforms to carry domestic Australian news content but would also require U.S. digital companies to transfer revenue to Australian competitors and disclose proprietary information related to private user data and algorithms. It explicitly and exclusively targets two U.S. companies without any indication of the selection criteria for these companies and their various services, or whether similar criteria was or will be applied to companies in or outside of Australia. (...) **In solely targeting U.S. companies, the Code conflicts with basic trade principles of national treatment and non-discrimination under the Australia-U.S. Free Trade Agreement (AUSFTA) and the WTO General Agreement on Trade in Services (GATS)."**
- **United States Council for International Business (October 2020):** "The proposed Code would interfere with the legitimate business decisions of two specific US digital platform businesses, and conveys unfettered discretionary power on the Australian Treasurer to designate other companies to which the Code should apply. (...) **The draft code, if enacted in its current form, would run counter to Australia's trade obligations in the over fifteen-year-old Australia-U.S. Free Trade Agreement (AUSFTA) as well as the WTO General Agreement on Trade in Services (GATS)**. It is also at odds with Australia's history of leadership in promoting cross-border digital trade."
- **Computer & Communications Industry Association (November 2020):** "Motivated by a desire to empower domestic news publishers, the new rules would dictate that online services negotiate and pay Australian news publishers for online content, and also disclose proprietary information related to private user data and algorithms. As drafted, the Australian Treasury would have the utmost discretion to determine which companies these mandates are applied to, and currently only two companies – both American – have been identified at this time. **There are significant concerns from a procedural, competition, trade, and intellectual property perspective that USTR should pay close attention to.**

In addition to submitting comments to the Australian Senate, these industry-backed groups used the NTE as a vehicle to attack the code and to recruit the U.S. government to help do so. Multiple trade associations that count Facebook and Google among their members listed the code as a violation of non-discrimination commitments in trade agreements. The now-shuttered Internet Association (IA) claimed in a NTE submission filed in October 2020 that *"The internet industry has strong concerns that the Code violates Australia's trade obligations and unfairly discriminates against U.S. companies. IA is expressly concerned that the Code targets two U.S. digital companies to assist a class of domestic players in a way that runs counter to Australia's international trade commitments."* [32] Five other industry associations joined the Internet Association in assailing the Australian media code proposal and urging USTR to intervene.

In response, in January 2021, USTR filed a submission before the Australian parliament asking it to *"suspend any plans to finalize this legislative proposal." In doing so, USTR argued that the code "explicitly and exclusively (as an initial matter) targets two U.S. companies through legislation without first having established a violation of existing Australian law or a market failure."* [33]

Leaving aside the fact that this submission by USTR is the perfect example of how industry groups use the NTE process in their assault against policies they dislike, a sovereign legislature does not need to prove that an existing law has been violated in order to pass or introduce a new one. If that were to

32 Comment from Internet Association, United States Trade Representative National Trade Estimate Report on Foreign Trade Barriers. Posted Oct. 30, 2020. Available at: https://www.regulations.gov/comment/USTR-2020-0034-0028. P. 21.

33 PDFs of all submissions regarding the code to the Australian Senate Standing Committee on Economics can be viewed at https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/TLABNewsMedia/Submissions.

be the case, neither the Sherman Act nor any other competition law would have been ever adopted. As for the assertion that the legislation targets two U.S. firms, competition and antitrust rules have long sought to principally rein in the outsized power of the most dominant firms. Antitrust cases by their very nature target specific firms that dominate their industries. This also means that when crafting laws, legislators have specific companies in mind, even if the policy intent is that no company, regardless of nationality, should have so much power. This is true in the United States as well, where, for example, the 1936 Robinson-Patman Amendment to the Clayton Antitrust Act was passed specifically with the dominant retailer A&P in mind.[34]

A year later, after the code was enacted, the Internet Association continued its assault in its 2021 NTE submission, listing Australia among foreign governments *"imposing or pursuing restrictive measures that target U.S. technology companies, leaving domestic competitors free to innovate."*[35]

Particularly with respect to the News Media legislation, it stated: *"USTR should continue to pay close attention to the implementation of the Code and its adherence to the principles of transparency, fairness and non-discrimination as consistent with the AUSFTA."*[36]

Facebook and Google both claimed to support the principle behind the code, but that did not stop either from punishing Australian consumers in retaliation as the legislation moved through parliament. Google threatened to pull its search function entirely from Australia. Facebook temporarily blocked access to news content in Australia. Facebook's block inadvertently also blocked several government resources, including

Other 2021 NTE Industry Attacks on the Australian News Media Code

- **Information Technology Industry Council (October 2021):** "While companies have not yet been designated, the Code accords the Australian Treasurer unfettered discretionary power to designate companies to which the Code should apply. **As the Code would only affect U.S. companies, it appears to conflict with basic trade principles of national treatment and non-discrimination under the Australia-U.S. Free Trade Agreement (AUSFTA) and the WTO General Agreement on Trade in Services (GATS).**" (emphasis added.)
- **Computer & Communications Industry Association (October 2021):** "Under the [Australian News Media Bargaining] Code, the Australian Treasury would have the utmost discretion to determine which companies these mandates are applied to by determining whether the platform holds significant bargaining power imbalance with Australia news media businesses. The Treasurer must also consider if the platform has made a significant contribution to the sustainability of the Australian news industry through agreements relating to news content of Australian news businesses. **Only two companies have been identified throughout deliberations. There are significant concerns from a procedural, competition, trade, and intellectual property perspective that USTR should pay close attention to. In particular, U.S. officials should monitor the implementation of the Code and its adherence to the principles of transparency, fairness and non-discrimination as consistent with the U.S.-Australia FTA**." (emphasis added.)

34 See Harry Ballan, "The Courts' Assault on the Robinson-Patman Act," Columbia Law Review, Vol. 92, No. 3, April 1992, pp. 635-636. Available at: https://www.jstor.org/stable/1122955?seq=2#metadata_info_tab_contents.

35 Comment from Internet Association, Request for Comments: Significant Foreign Trade Barriers for the National Trade Estimate Report. Posted Oct. 28, 2021. Available at: https://www.regulations.gov/comment/USTR-2021-0016-0064.

36 Comment from Internet Association, Request for Comments: Significant Foreign Trade Barriers for the National Trade Estimate Report. Posted Oct. 28, 2021. Available at: https://www.regulations.gov/comment/USTR-2021-0016-0064. P. 6 and 14.

emergency services pages, and charities, a move which sparked local support for the code among Australians frustrated by corporate bullying.[37]

However, as imminent passage of the code approached in 2021, Google and Facebook both signed separate deals with several of Australia's largest publishers and smaller, regional, and digital-only platforms to avoid use of the legislation. The terms of these deals are deemed as commercial in confidence, meaning it is unknown how much money outlets are paid and how newsrooms use that money. Yet, the Australian Treasurer estimates that a total of over AU$200 million (about $140 million USD) has been paid to news media companies in the year since the law was enacted, and news companies have already announced increased staffing and rural coverage as a direct result of the new funds received from the deals with Big Tech.[38]

To that extent, the clear market failure that the Australian code spotted was successfully resolved. Dominant digital platforms have been profiting immensely off of the work of publishers who are not compensated for the work that they do. Australian journalism, like journalism elsewhere in the world, had been struggling for decades. But, after the new code last year, the Australian news media has been injected with millions of dollars, and hiring of journalists has significantly recovered.[39]

The European Approach to Digital Markets Regulation Under Assault: The Digital Markets Act and Digital Services Act

As their role in society has grown, a small number of digital platforms have gained a dominant position that allows them to crush competitors and exert sole control over consumer choices, often to consumers' detriment. Standard competition policy has been criticized as ineffective to keep up with changing market realities in light of new technologies and practices in the digital age. While existing antitrust and competition rules already prohibit many forms of anticompetitive behavior that appear to be common in digital markets, the enforcement of these rules has been lackluster.

37 Nick Baker, "Outrage as Facebook blocks access to news content in Australia," NBC News, Feb. 18, 2021. Available at: https://www.nbcnews.com/tech/tech-news/outrage-facebook-blocks-access-news-content-australia-rcna297

38 Bill Grueskin "Australia pressured Google and Facebook to pay for journalism. Is America next?" Columbia Journalism Review, March 9, 2022. Available at: https://www.cjr.org/business_of_news/australia-pressured-google-and-facebook-to-pay-for-journalism-is-america-next.php

39 Anya Schiffrin, "Australia's news media bargaining code pries $140 million from Google and Facebook," Poynter, Aug. 16, 2022. Available at: https://www.poynter.org/business-work/2022/australias-news-media-bargaining-code-pries-140-million-from-google-and-facebook/.

To prevent abuse of market power by the largest digital platforms in European Union countries and protect competition in European digital markets, the European Union designed twin legislation: The Digital Markets Act (DMA) and the Digital Services Act (DSA), which together create a single set of rules spanning the EU.

The Digital Markets Act establishes a list of obligations for designated gatekeepers and sanctions for gatekeepers who fail to comply.[40] The DMA regulates certain behaviors that could reduce competition in digital markets ex ante, or before they happen, alongside traditional antitrust legislation.

Companies can be deemed gatekeepers if they provide services in one of eight different areas called Core Platform Services and have a significant impact on the European market. These areas include online search engines, online intermediation services, social networks, video sharing platforms, communications platforms, advertising systems, operating systems, and cloud services.[41] Plus, to be considered a gatekeeper, companies must have at least 45 million monthly active users and more than 10,000 active business users in the EU, as well as a market capitalization of at least €75 billion or an annual European turnover equal to or above €7.5 billion for three years in a row.[42]

Under the DMA, gatekeepers must follow a list of "dos" and "don'ts." Gatekeepers' new obligations include: [43]

1. A prohibition from self-preferencing proprietary systems or having discriminatory ratings for competitor services and products.
2. A ban from combining data collected from different services owned by a single company.
3. A prohibition from setting proprietary software as the default option when users set up devices.
4. A requirement to ensure interoperability with smaller digital platforms and data portability.
5. An obligation to meet advertisement pricing transparency guidelines.

40 Morgan Meaker, "Europe's Digital Markets Acts Takes a Hammer to Big Tech," Wired, March 25, 2022. Available at: https://www.wired.com/story/digital-markets-act-messaging/.

41 Questions and Answers: Digital Markets act: Ensuring fair and open digital markets, European Commission. Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2349; Mario Mariniello and Catarina Martins (2021) 'Which platforms will be caught by the Digital Markets Act? The 'gatekeeper' dilemma', Bruegel Blog, 14 December. Available at: https://www.bruegel.org/blog-post/which-platforms-will-be-caught-digital-markets-act-gatekeeper-dilemma.

42 Ryan Browne, "EU targets US tech giants with a rulebook aimed at curbing their dominance," CNBC, March 25, 2022. Available at: https://www.cnbc.com/2022/03/25/digital-markets-act-eu-targets-big-tech-with-sweeping-new-antitrust-rules.html.

43 Questions and Answers: Digital Markets act: Ensuring fair and open digital markets, European Commission. Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2349

In essence, gatekeepers must operate according to rules that aim to create a level playing field in the market for all digital companies – from mega platforms to start-ups.

While designed to update European regulations to the digital age, each of these provisions has analogues in either longstanding American laws and regulations or current American proposals for similar rules. For each of the DMA provisions in turn:

1. Prohibiting platforms from self-preferencing their own products via their platform is the aim of the American Innovation and Choice Online Act, currently awaiting a vote in the U.S. Senate after being approved in committee.[44]

2. Prohibiting the combinations of collected data between business subdivisions has been a frequently considered remedy for mergers in the past 10 to 15 years in the United States, even as technology firms have frequently violated such promises when they have informally made them.[45]

3. The pre-installation and integration of proprietary software was the exact topic of the 1990s American litigation against Microsoft. The company was initially found to have abused an illegal tie-in by integrating Internet Explorer (IE) with Windows and foreclosing competition for browsers.[46] Even though Microsoft had a more favorable ruling on appeal, the appellate court nonetheless found that Microsoft violated Section 2 of the Sherman Act by integrating IE and Windows.[47]

4. Interoperability, while a term specifically for digital markets, refers to relatively mundane regulatory practices of setting standards for products, services, processes, and systems. The American National Bureau of Standards was founded in 1901, and it continues to this day as the National Institute of Standards and Technology.

5. The United States has consumer protection rules around transparency in advertising specific to digital markets. The FTC outlined their requirements for online advertising in 2000[48] and 2013,[49] clarifying that the same standards for consumer protections that are used offline also apply in digital markets. The FTC is likewise currently undergoing a rulemaking process to update their guidance on advertising disclosures in digital markets.[50]

44 S.2992 – 117th Congress (2021-2022): American Innovation and Choice Online Act. Available at: https://www.congress.gov/bill/117th-congress/senate-bill/2992/text

45 Most notably, in 2016, Google merged its own data with that of DoubleClick after its 2007 acquisition, despite having promised Congress that it would not do so.

46 United States v. Microsoft Corp., 87 F. Supp. 2d 30 (D.D.C. 2000).

47 U.S. v. Microsoft Corp., 253 F.3d 34 (D.C. Cir. 2001).

48 "Dot Com Disclosures," Federal Trade Commission. Available at: https://www.ftc.gov/sites/default/files/attachments/press-releases/ ftc-staff-issues-guidelines-internet-advertising/0005dotcomstaffreport.pdf.

49 ".com Disclosures: How to Make Effective Disclosures in Digital Advertising," Federal Trade Commission, March 2013. Available at: https://www.ftc.gov/system/files/documents/plain-language/bus41-dot-com-disclosures-information-about-online-advertising.pdf.

50 "FTC Staff Requests Information Regarding Digital Advertising Business Guidance Publication," 2022. Available at: https://www.ftc.gov/system/files/ftc_gov/pdf/Digital%20Advertising%20Business%20Guidance%20Request%20for%20Information.pdf.

The Digital Services Act focuses on granting consumers greater control over the content they see online and better protections from abuses by dominant corporations. Unlike the DMA, the DSA applies to all digital services, defined as "a large category of online services, from simple websites to internet infrastructure services and online platforms" that operate in the EU, regardless of size or where the business is actually located.[51] More specifically, the DSA regulates digital services that connect consumers with goods, other services, and content.

The DSA provides better user protections, creates a set of user rights online, and establishes a transparency and accountability framework for algorithms and terms and conditions on online platforms. As with the DMA, the DSA establishes obligations and prohibitions for digital companies. For example, the DSA bans so-called 'dark patterns' that confuse and mislead users into making unintended choices and prohibits targeted advertising based on protected categories like race or religion. It also includes new measures to monitor illegal content online, obligations to mitigate risks of disinformation, election manipulation, or cyberviolence against women and minors on online platforms, and transparency standards to protect consumers in online marketplaces.[52] In essence, the DSA deals with the way online platforms handle the content they host and more directly protects users.

The DSA and DMA also come with strict enforcement mechanisms. In the case of the DMA, a single violation could result in a fine of up to 10% of a company's global revenue. Repeated violations can result in fines up to 20% of a company's global revenue. Three violations in less than eight years could result in a market investigation and structural remedies, including potential breakup.[53]

Big Tech companies have made a concerted effort to portray the DMA as a legislative strategy whose main target is undermining the competitiveness of American firms – this despite so many elements of the policy having U.S. counterparts.

Big Tech friendly groups have argued that the DMA is a form of discriminatory tech protectionism that would restrict market access for U.S. tech firms in Europe and could violate WTO commitments by benefiting European companies at the deliberate expense of American firms.[54] A bipartisan group of lawmakers, led by Reps. Suzan DelBene (D-Wash.) and Darin LaHood (R-Ill.) and including other Big Tech friendly legislators like Rep. Zoe Lofgren (D-Cal.) wrote a letter to President Biden in early 2022 stating that the DMA uses deliberately discriminatory and subjective thresholds to designate U.S. tech

51 The Digital Services Act package, European Commission. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

52 Questions and Answers: Digital Services Act, European Commission. Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348.

53 Ryan Browne, "EU targets US tech giants with a rulebook aimed at curbing their dominance," CNBC, March 25, 2022. Available at: https://www.cnbc.com/2022/03/25/digital-markets-act-eu-targets-big-tech-with-sweeping-new-antitrust-rules.html.

54 Meredith Broadbent, "Implications of the Digital Markets Act for Transatlantic Cooperation," CSIS, Sept. 15, 2021. Available at: https://www.csis.org/analysis/implications-digital-markets-act-transatlantic-cooperation

firms as gatekeepers.[55] High-level Big Tech friendly Biden administration officials, such as Commerce Secretary Gina Raimondo, publicly criticized the DMA and DSA, repeating the industry claims that the policies target American companies.[56]

A 2021 paper prepared by corporate law firm King and Spalding for the Computer and Communications Industry Association, a U.S. group including Amazon, Apple, Facebook, Google, Intel, and Twitter, argues that the DMA violates WTO most favored nation and national treatment rules by targeting and discriminating against U.S. companies.[57] The paper contends that the DMA de facto grants less favorable treatment to U.S. companies in ways that do not apply to European companies, and argues that this is a violation of the GATS. In multiple statements, the U.S. Chamber of Commerce has denounced both the DMA and the DSA as discriminatorily targeting American companies based solely on their success.[58]

These "trade discrimination" claims pay little attention to the fact that, based on the thresholds ultimately established, the DMA would include at least three European companies as meeting the requirements to be considered a digital gatekeeper.[59] While launching these broad attacks on both policies, industry groups also fail to mention that the DSA obligations apply to all firms that provide digital services in the EU and, unlike the DMA, there are no quantitative thresholds for its application.

55 Lauren Feiner, "Bipartisan lawmakers want Biden to tell Europe to stop 'unfairly' targeting US tech companies," CNBC, Feb. 23, 2022. Available at: https://www.cnbc.com/2022/02/23/lawmakers-ask-biden-to-tell-eu-to-stop-unfairly-targeting-us-tech-companies.htm

56 Jorge Liboreiro, "*EU and US vow to boost microchip supplies and promote trustworthy AI*," Euronews, Jan. 10, 2021. Available at: https://www.euronews.com/my-europe/2021/09/30/eu-and-us-vow-to-boost-microchip-supplies-and-promote-trustworthy-ai.

57 'The EU Digital Markets Act Targets Discrimination Against US Companies in Violation of WTO Commitments and Threatens the Re-Set of Trade Multilateralism and of Trans-Atlantic Relations,' King and Spalding LLC, June 8, 2021. Available at: https://www.kslaw.com/attachments/000/008/860/original/EU_Digital_Markets_Act_-_Trade_law_and_systemic_implications_8_June_2021.pdf?1624300896.

58 US Chamber Concerned by European Commission Digital Services and Digital Markets Proposals, Dec. 15, 2020. Available at: https://www.uschamber.com/technology/us-chamber-concerned-european-commission-digital-services-and-digital-markets. See also: 'The EU's Proposed Digital Market's Act: Key Concerns and Recommended Adjustments.' Available at: https://www.uschamber.com/international/the-eus-proposed-digital-markets-act-key-concerns-and-recommended-adjustments.

59 Considering that under the higher thresholds proposed in December 2021 by the European Parliament's Internal Market and Consumer Protection Committee, Germany's SAP, Netherlands' Booking, and France's Vivendi would have been covered, it is clear that the final legislation includes these European companies. See Mario Mariniello and Catarina Martins (2021) 'Which platforms will be caught by the Digital Markets Act? The 'gatekeeper' dilemma', Bruegel Blog, 14 December. Available at: https://www.bruegel.org/blog-post/which-platforms-will-be-caught-digital-markets-act-gatekeeper-dilemma.

Big Tech-funded groups once again used the NTE to attack the DMA and DSA. The first NTE submissions criticizing these pieces of legislation came in even before there was clarity about the precise aim of each of the proposals. A submission by the U.S. Council for International Business filed in November 2020 shows that industry groups started assaulting the twin legislation even before knowing their different reach and objectives: "*Most significantly, as part of the Digital Services Act, the European Commission proposes an ex ante regime to control behavior of 'large online platforms' designated as 'gatekeepers.' Such firms, broadly anticipated to be mostly US firms, could be forced to share data with competitors and be restrained from certain conduct that is common certain conduct that is common across many economic sectors, regardless of specific evidence or proven harm*."[60]

When the European Commission finally unveiled the text of the legislative proposals in December 2020, U.S. industry groups' attacks intensified, with organizations like the Computer & Communications Industry Association writing in a 2021 NTE comment that the DMA's "*thresholds have been set at levels where primarily US technology companies will fall under scope," and that "(t)he list of "core platform services" furthermore carves out non-platform-based business models of large European rivals in media, communications, and advertising*."[61]

The U.S. Council for International Business went a step further in its 2021 NTE submission, claiming that: "*These unilateral regulations [the DMA and DSA] appear designed to discriminate against U.S. companies and to take aim at a slice of the $517 billion U.S. digital export market. (...) As the EU considers structural measures to address the digital marketplace, we urge USTR to work with the EU to ensure that it does not discriminate against U.S. companies through its laws and regulations, and that it upholds principles of non-discrimination, regulatory transparency, and technology neutrality in laws and regulations*."[62]

60 Comment from U.S. Council for International Business Regarding Foreign Trade Barriers to U.S. Exports for 2020 Reporting, page 48. Posted Oct. 27, 2020. Available at: https://www.regulations.gov/comment/USTR-2020-0034-0015.

61 Comment from Computer & Communications Industry Association, USTR National Trade Estimate Report on Foreign Trade Barriers. Posted Oct. 28, 2021. Available at https://www.regulations.gov/comment/USTR-2021-0016-0049.

62 Comment from U.S. Council for International Business, USTR National Trade Estimate Report on Foreign Trade Barriers. Posted Oct. 28, 2021. Available at https://www.regulations.gov/comment/USTR-2021-0016-0042.

Other NTE Industry Attacks on the DMA/DSA

- **Internet Association (October 2021):** "The European Commission published its Digital Markets Act (DMA) proposal in December 2020. **The DMA includes an array of extraordinary prohibitions that will apply exclusively to a small group of U.S. platforms**. EU officials have been clear that they aim to use the DMA to reduce "dependence" on U.S. services and to support local industry, furthering the EU's current agenda of digital sovereignty.
  As proposed, the DMA would impose sweeping competitive restrictions on companies labeled as "gatekeepers," which the EU has defined narrowly to refer to a specific subset of U.S. technology providers, while excluding European digital rivals and other EU industries that compete with the U.S. technology sector. If enacted, US companies would be forced to comply with new obligations and regulatory restrictions that would damage their competitiveness with foreign firms, while the EU – as well as Russia, China, and other foreign rivals – would be entirely free of these restrictions." (emphasis added).
- **Information Technology Industry Council (October 2021):** " (...) previous proposals have progressed through the legislative process. These include the bloc's new rules for online platforms in the Digital Services Act (DSA), the new Digital Markets Act (DMA), which sets out to address the challenges posed by "gatekeepers," and new rules for re-use of sensitive data held by the tech sector in the Data Governance Act (DGA).
  ITI is closely involved in these legislative procedures and continues to underscore the need for the EU to pursue its policy objectives in a manner that eschews protectionism and discrimination." (emphasis added)
  "**Concerns remain that the DMA's application may be limited to a handful of primarily U.S.-headquartered firms.** The DMA is currently being amended in parallel by the Council of the EU and the European Parliament, with a final deal expected in 2022. **ITI encourages USTR and the U.S. administration to engage with the EU to ensure that the rules are targeted to proven and clear market failures and remain non-discriminatory in nature.** We also continue to advocate for the establishment of a regulatory dialogue in the context of the DMA to ensure that rules are fairly and transparently applied." (emphasis added)
- **Coalition of Services Industries (October 2021):** "In December 2020 the European Commission issued the Digital Markets Act, a complex proposal that seeks to impose new restrictions on large online service providers, deemed "gatekeepers," in the name of promoting competition. **The scope of the law could impact U.S. companies disproportionately**.
  As the EU considers structural measures to address the digital marketplace, **we encourage USTR to work with the EU to uphold principles of non-discrimination and technology neutrality in laws and regulations. It is important that regulatory approaches impacting digital services and technologies are not protectionist, but rather developed in a deliberate and consultative manner subject to traditional trade principles, including non-discrimination and national treatment**."

Big Tech's pressure on the U.S. government has been relatively effective. Although USTR Tai has refrained from attacking these European initiatives and the 2022 NTE report merely included a description of the DMA and DSA,[63] this has not been the case with other parts of the administration. Certain U.S. officials from other agencies have continuously pressed the EU and repeated digital mega-platforms' erroneous claims that the DMA is designed to target only U.S. firms, including through the EU-US Trade and Technology Council. These officials have gone even further, suggesting reducing the scope of services covered, lowering the amount of fines to be imposed to violating firms, and extending the timeframe to implement the legislation.[64]

63 2022 National Trade Estimate Report on Foreign Trade Barriers, pages 216-217. Available at: https://ustr.gov/sites/default/files/2022%20National%20Trade%20Estimate%20Report%20on%20Foreign%20Trade%20Barriers.pdf

64 Samuel Stolton, "US pushes to change EU's digital gatekeeper rules," Politico, Jan. 31, 2022. Available at: https://www.politico.eu/article/us-government-in-bid-to-change-eu-digital-markets-act/.

Ultimately, the DMA was adopted in July 2022[65] and the DSA a couple of months later in October.[66] Yet, the fact that some U.S. officials have answered Big Tech's call to attack these policies in Europe has served industry's interests in the United States. U.S. officials' public criticism of the DMA has been leveraged to try to undermine similar legislative proposals making their way through the U.S. Congress. For instance, the U.S. Chamber of Commerce argues that "the White House needs to read its own talking points [regarding the DMA], before it takes a final position on the legislation [the American Innovation and Choice Online Act]. Providing support for similarly misguided domestic bills, the administration could transform the world's most innovative economy into one that reeks of stagnation."[67]

Germany Revamps its Competition Policy to Counter Big Tech Abuses

The DMA and DSA will apply to Germany as a member of the EU. However, after several antitrust investigations of digital platforms by the German Federal Cartel Office (FCO), in January 2021 Germany passed its own version of the DMA with amendments to the German Act Against Restraints of Competition, also known as the GWB Digitization Act.[68] These amendments made Germany the first country in the world with preventative rules to regulate abuse of market dominance by large digital platforms.

Like the DMA, the GWB Digitization Act allows the FCO to prohibit certain "super dominant firms" from engaging in certain anticompetitive behaviors. These behaviors include self-preferencing, using competitively relevant data in a way that raises barriers to market entry, impeding interoperability, expanding the dominant position to a new market, or providing insufficient information about services.

"Super dominant firms" are those that have "overwhelming importance for competition across multiple markets."[69]

65 "Digital Markets Act: European Union Adopts New "Competition" Regulations for Certain Digital Platforms," JDSupra, Aug. 3, 2022. Available at: https://www.jdsupra.com/legalnews/digital-markets-act-european-union-5708655/.

66 DSA: Council gives final approval to the protection of users' rights online. Oct. 4, 2022. Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/10/04/dsa-council-gives-final-approval-to-the-protection-of-users-rights

67 "Striking Similarities: Comparing Europe's Digital Markets Act to the American Innovation and Choice Online Act," U.S. Chamber of Commerce. June 17, 2022. Available at: https://www.uschamber.com/finance/antitrust/striking-similarities-dma-american-innovation-act.

68 'Germany Adopts New Competition Rules for Tech Platforms,' Jones Day, January 2021. https://www.jonesday.com/en insights/2021/01/germany-adopts-new-competition-rules

69 "Germany Adopts New Competition Rules for Tech Platforms," Jones Day, Jan. 2021. Available at: https://www.jonesday.com/en/insights/2021/01/germany-adopts-new-competition-rules.

The GWB Digitization Act also includes major reforms to Germany's competition policy framework, including:[70]

1. A revamped definition of dominance that includes intermediary power (control over access to supply and sales markets) as a factor to analyze when determining if a firm is dominant.
2. Limits on dominant firms from using certain behaviors that can lead markets to "tip" into monopolistic structures.
3. A prohibition forbidding dominant firms from denying access to "essential facilities," which could include access to data.
4. New powers to issue "interim measures" to halt certain business practices, which are likely to be anticompetitive, before an antitrust probe concludes.

In sum, the amendments to the German competition regime aim at preventing mega platforms from using their outsized position in the digital space to box out smaller competitors.

Again, corollaries to these provisions exist or have existed in American law, and as such it is difficult to frame them as discriminatory against American companies. Some of these principles include:

1. American law includes and has included many different tests to determine whether a firm is a monopoly or has market power. New York State's proposed "21st Century Antitrust Act" includes an abuse-of-dominance standard that incorporates many different tests to determine if a firm is dominant, including market shares as either a buyer or seller, as well as direct evidence of like the power to unilaterally set contract terms of prices.[71] The proposed Competition and Antitrust Law Enforcement Reform Act of 2021 likewise uses a combination of factors to determine whether a company has market power.[72]
2. American antitrust policy prohibits the anticompetitive leveraging of dominance in one market to attain a monopoly in another.[73]

70 'Major Amendments to German Act Against Restraints of Competition Take Effect,' JDSupra, Jan. 25, 2021. https://www.jdsupra.com/legalnews/major-amendments-to-german-act-against-1056069/; 'Germany Adopts New Competition Rules for Tech Platforms,' Jones Day, January 2021. https://www.jonesday.com/en/insights/2021/01/germany-adopts-new-competition-rules

71 Senate Bill S933C, https://www.nysenate.gov/legislation/bills/2021/s933/amendment/c.

72 S.225 - Competition and Antitrust Law Enforcement Reform Act of 2021. Available at: https://www.congress.gov/bill/117th-congress/senate-bill/225/text

73 Although the doctrine of monopoly leveraging has been weakened over time, American antitrust law does recognize that is illegal to leverage monopoly power in one market to obtain dominance in another. Berkey Photo, Inc. v. Eastman Kodak Company, 603 F.2d 263, 275 (2d Cir. 1979) ("[A] firm violates [Section 2 of the Sherman Act] by using its monopoly power in one market to gain a competitive advantage in another, albeit without an attempt to monopolize the second market.")

3. While significantly weakened in recent decades, essential facilities doctrine has its origins in American antitrust law, going back to the Supreme Court's 1912 Terminal Railroad decision.[74]

4. While the German proposals for "interim measures" are a new form of enforcement, they are not categorically different from American courts issuing preliminary injunctions, which are occasionally used in antitrust cases.[75]

Like the DMA, the German approach has been attacked in NTE submissions by industry-backed groups as protecting domestic companies by discriminating against American technology firms based on their size and market dominance.[76] In its 2022 comment, the Computer & Communications Industry Association directly called the amendments a trade barrier and claimed that they *"were written to be enforced solely against US companies" and "are starkly inconsistent with longstanding US and global competition norms."*[77]

Other NTE Industry Attacks on the GWB Digitization Act

- **Internet Association (October 2021):** Under the "Discriminatory Or Opaque Application Of Competition Regulations" heading: "A new competition law entered into force in Germany in January 2021 that allows the German Federal Cartel Office ("FCO") to subject certain companies to prohibitions and penalties even if there has been no showing of an abuse of a dominant market position, which would be flatly inconsistent with U.S., EU and global practice. The companies targeted are online platforms and other companies that German authorities accuse of "transcending" their market power in a given market because, for example, they are vertically integrated or control sensitive business data. After the new law became effective, the FCO immediately used its new powers and initiated investigations against US-based companies Facebook, Google, Amazon, and Apple alleging that these companies are of "paramount significance for competition across markets."
  Other rules in the new law also target online platforms, including a rule that makes it easier for competition authorities to oblige platforms to provide access to data. Many of the rules include fuzzy definitions of longstanding concepts in competition law (such as "essential facilities") and depart from global competition norms, including by shifting the burden of proof away from the FCO and towards targeted companies. **Together these rules come close to introducing a sector-specific regulation of online platforms by means of antitrust law and could serve as a model for other countries worldwide that are looking to challenge or undermine U.S. businesses operating in this sector**. Overall, the new regime is likely to negatively affect U.S.-German digital trade."
- **Computer & Communications Industry Association (November 2020):** Germany is currently in the process of reforming its competition rules, with a draft bill introduced in 2020. Reports indicate that a central part of the reform will be to "move to a preventative level (ex ante) imposing precautionary antitrust responsibilities on companies rather than waiting for an abuse to take place before taking action." German authorities have also proposed targeting online platforms and other companies supposedly "transcend" their dominance in a given market based on vertical integration concerns or access to sensitive data. Another proposed rule would shift the burden of proof away from competition authorities and towards targeted companies. **Many of these proposals are starkly inconsistent with longstanding U.S. and global competition norms and, if adopted, could serve as trade barriers.**

74 *United States v. Terminal Railroad Association*, 224 U.S. 383 (1912).

75 For example, see: natlawreview.com/article/second-circuit-affirms-preliminary-injunction-antitrust-suit-against-drug-companies.

76 'On the Rise: Europe's Competition Policy Challenges to Technology Companies,' CSIS, Oct. 26, 2020. https://www.csis.org/analysis/rise-europes-competition-policy-challenges-technology-companies

77 Comment from Computer & Communications Industry Association, Request for Comments: Significant Foreign Trade Barriers for the National Trade Estimate. Posted Oct. 28,2021. Available at: https://www.regulations.gov/comment/USTR-2021-0016-0049.

In the year and a half since the GWB Digitization Act came into force, the FCO has found that Meta, Google,[78] and Amazon[79] are of "paramount significance across markets," meaning that they must comply with the stricter new regulations. Apple is currently also under review by the FCO.

Conclusion

As policymakers in the United States and around the world have begun introducing policies to rein in the mega-platforms dominating the digital economy, Big Tech is employing every trick in the book to fight these efforts. This includes trying to co-opt trade concepts and trade negotiations in a stealthy attack on cutting-edge digital governance policies around the world. Their goal is to rig trade rules so as to get key digital governance tools labeled as illegal trade barriers even though these policies have nothing to do with trade.

This report shows Big Tech interests are trying to hijack the international trade law concept of non-discrimination and redirect it to push their own agenda of avoiding regulation and maintaining their dominant positions and monopolistic behavior. The trade non-discrimination standard is in theory meant to equalize treatment of foreign and domestic goods. But runaway trade tribunals and various commercial interests have worked to expand the trade non-discrimination standard to include facially neutral policies that may have disproportionate effects. Now Big Tech is seeking to exploit this expanded definition to claim that origin-neutral policies that may have a larger impact on the largest firms due simply to their size are discriminatory illegal trade barriers. Put simply, industry groups backed by Big Tech have taken to calling foreign digital governance policies that they do not like trade barriers in order to mask their real objection, which is to being regulated, despite their endless abuses.

This report documents instances of industry use of such claims in the context of the annual National Trade Estimates process to attack foreign policies they dislike. More than seven industry associations launched 30 attacks using "non-discrimination" trade lingo against four policy initiatives that other countries have employed to create more competitive digital markets. A significant number of them were successful in mobilizing U.S. officials against other nations' digital competition policies. The most salient case is related to the Australian News Media Bargaining Code since, following the scalding 2021 NTE submissions of more than five industry associations, USTR filed a submission before the Australian parliament criticizing the legislation and demanding the suspension of any plans to finalize the proposal. These attacks against foreign policies, in turn, have served

78 Laura Kabelka, "German competition authority tightens grip on Meta," EURACTIV.dc. Available at: https://www.euractiv.com/section/digital/news/german-antitrust-body-to-adopt-stricter-measure-against-meta/.

79 Laura Kabelka, "Germany's antitrust body tightens grip on Amazon over market dominance," EURACTIV.de. Available at: https://www.euractiv.com/section/digital/news/germanys-anitrust-body-tightens-grip-on-amazon-over-market-dominance/.

Big Tech's strategy against key legislative proposals in the United States that replicate these foreign initiatives.

The tone of the Biden administration National Trade Estimate reporting is less hostile to the concept of digital governance even as some of the policies noted in this report are described, albeit without the hostile comments included in past NTE editions.

Previous NTEs included language so friendly to Big Tech that the mega-platforms repurposed it for their own statements and subsequent NTE submissions. An example of this practice is the way in which the Coalition of Services Industries and the Internet Association adopted the exact same language that USTR used in its 2021 report to criticize the Korean App Store Law when they filed their NTE submissions later that same year.

Big Tech's agenda to restrict governments' abilities to constrain their monopolistic power and anticompetitive behavior is consistent, but political leadership is subject to change. Policymakers must be aware of Big Tech's hijacking of trade concepts such as non-discrimination, also called "national treatment", to block domestic policymaking and continue to expand their power.

The industry NTE submissions detailed in this report make clear how Big Tech interests are willing to manipulate "non-discrimination" notions in trade lingo in order to attack digital governance policies around the world. To safeguard both domestic and foreign policymakers' ability to protect consumers, workers, and small businesses from monopolistic abuses by mega-platforms, it is critical that any "non-discrimination" obligations included in agreements related to the digital economy are narrow and only capture policies whose main objective is discriminating against foreign rivals. If vague "non-discrimination" obligations are included in bilateral, regional, and multilateral "digital trade" agreements, Big Tech will continue to weaponize trade jargon and trade-pact enforcement to attack pro-competition and pro-consumer policies worldwide, further undermining the legitimacy of trade agreements.

List of Industry Association NTE Submissions Attacking Digital Competition Policies

I. Industry Submissions to the 2021 National Trade Estimate Report

a. Korea's App Store Law

i. Information Technology Industry Council: "In October 2020, Korean legislators in the National Assembly proposed six bills that would amend the Telecommunications Business Act to ban app stores from requiring that app developers use a uniform billing system. **While the proposals appear origin-neutral on the surface, Korean legislators have made clear through public statements that the legislative intent is to target U.S. firms, while favoring their Korean competitors. If enacted into law, the legislative proposals would restrict U.S. app stores' ability to charge a service fee through their own payment platforms, thereby limiting the ability to provide services in a safe, secure, and efficient way.** Industry is concerned that the conditions imposed on U.S. companies by the proposed amendments would significantly impede affected companies' ability to supply global services on a cross-border basis to Korea, and would potentially run afoul of Korean market access and investment commitments under the Korea-United States Free Trade Agreement (KORUS). The conditions would also restrict U.S. app developers' ability to reach the Korean market via trusted U.S. ecosystems." (pg.48) *(emphasis added)*

b. Australia's News Media Bargaining Code

i. ***Internet Association:*** **"The internet industry has strong concerns that the Code violates Australia's trade obligations and unfairly discriminates against U.S. companies. IA is expressly concerned that the Code targets two U.S. digital companies to assist a class of domestic players in a way that runs counter to Australia's international trade commitments.** The ACCC's proposed Code would improperly require proprietary information sharing by U.S. digital platforms without transparent standards or safeguards, and would set a dangerous precedent of political interference in Australia's digital economy. Finally, the Code presents an unfair and arbitrary treatment of foreign investors. Given the wide ramifications, we believe the ACCC should reconsider its proposed legislation and pursue a balanced solution for Australia's digital economy and consumers. **The draft code, if enacted in its current form, would run counter to Australia's trade obligations in the over fifteen-year-old AUSFTA as well as the WTO General Agreement on Trade in Services (GATS).** It is also at odds with Australia's history of leadership in promoting cross-border digital trade." *(pg. 21) (emphasis added)*

ii. ***Information Technology Industry Council:*** "In August 2020, the Australia Competition and Consumer Commission released a Draft Media Bargaining Code to address perceived imbalances in financial arrangements between news media publishers and digital

platforms that may feature news content. The Code not only requires digital platforms to carry domestic Australian news content but would also require U.S. digital companies to transfer revenue to Australian competitors and disclose proprietary information related to private user data and algorithms. **It explicitly and exclusively targets two U.S. companies without any indication of the selection criteria for these companies and their various services, or whether similar criteria was or will be applied to companies in or outside of Australia.** The Code also accords the Australian Treasurer with unfettered discretionary power to designate other companies to which the Code should apply. **The draft Code would impose discriminatory and burdensome responsibilities on U.S. companies where Australian, Chinese, Japanese, European, or other third-country technology businesses would not incur the same responsibilities. In solely targeting U.S. companies, the Code conflicts with basic trade principles of national treatment and non-discrimination under the Australia-U.S. Free Trade Agreement (AUSFTA) and the WTO General Agreement on Trade in Services (GATS).”** *(pg. 6) (emphasis added)*

iii. ***U.S. Council for International Business:*** **“The proposed Code would interfere with the legitimate business decisions of two specific US digital platform businesses**, and conveys unfettered discretionary power on the Australian Treasurer to designate other companies to which the Code should apply. The Code not only requires digital platforms to carry domestic Australian news content but would also require U.S. digital companies to transfer revenue to Australian competitors and disclose proprietary information related to private user data and algorithms. **The draft code, if enacted in its current form, would run counter to Australia’s trade obligations in the over fifteen-year-old Australia-U.S. Free Trade Agreement (AUSFTA) as well as the WTO General Agreement on Trade in Services (GATS).** It is also at odds with Australia’s history of leadership in promoting cross-border digital trade.” *(pg. 4-5) (emphasis added)*

iv. ***Computer and Communications Industry Association:*** **“Motivated by a desire to empower domestic news publishers,** the new rules would dictate that online services negotiate and pay Australian news publishers for online content, and also disclose proprietary information related to private user data and algorithms. As drafted, the Australian Treasury would have the utmost discretion to determine which companies these mandates are applied to, and **currently only two companies – both American – have been identified at this time. There are significant concerns from a procedural, competition, trade, and intellectual property perspective that USTR should pay close attention to.**” *(pg. 19) (emphasis added)*

v. ***Coalition of Services Industries:*** **“The proposed Code would interfere with the legitimate business decisions of two specific US digital platform businesses** and confer unfettered discretionary power on the Australian Treasurer to designate other companies to which the Code should apply. The Code not only requires digital platforms to carry domestic Australian news content but would also require U.S. digital companies to transfer revenue to Australian competitors and disclose proprietary information related to private user data and algorithms. **The draft code, if enacted in its current form,**

would run counter to Australia's trade obligations in the over fifteen-year-old Australia-U.S. Free Trade Agreement (AUSFTA) as well as the WTO General Agreement on Trade in Services (GATS). It is also at odds with Australia's history of leadership in promoting cross-border digital trade." *(pg. 7) (emphasis added)*

vi. ***National Foreign Trade Council:*** **"Over the past year, some foreign governments have also devised new ways of targeting U.S. digital companies and reducing their space to operate in foreign markets while protecting their domestic industries.** One particular example of concern is Australia's draft News Media and Digital Platforms Mandatory Bargaining Code which would require U.S. digital companies to carry domestic Australian news content, transfer revenue to Australian competitors and disclose proprietary information related to private user data and algorithms." *(pg. 6-7) (emphasis added)*

c. EU's Digital Markets Act/Digital Services Act

i. ***U.S. Council for International Business:*** **"Most significantly, as part of the Digital Services Act, the European Commission proposes an ex ante regime to control behavior of 'large online platforms' designated as 'gatekeepers'. Such firms, broadly anticipated to be mostly US firms, could be forced to share data with competitors and be restrained from certain conduct that is common across many economic sectors, regardless of specific evidence or proven harm.** In the context of the proposal the EU policymakers further suggest the establishment of a new EU regulator to oversee and enforce rules. **While Europe wants to tighten competition rules and enforcement for US tech firms, the EU is also seeking to loosen competition rules for EU industrial champions.** *(pg. 37-38) (emphasis added)*

ii. ***Internet Association:*** "Since the European elections in 2019, EU leaders have actively promoted a multi-pronged approach towards "technological sovereignty" or "digital sovereignty" as a main policy objective. In updates to the EU's digital and industrial agenda calls for "technology sovereignty" have been advanced with regards to data, artificial intelligence, cloud services, as well as on the responsibility of online platforms and competition policy with the latter two packaged as the Digital Services Act and Digital Markets Act.

While the precise meaning of sovereignty or autonomy in the realm of technologies remains ambiguous, EU leaders have emphasized the desire to limit the market position of U.S. providers. For example, some EU officials have called for a range of policies to support "a European way of digitization, to reduce our dependence on foreign hardware, software and services."

A recent draft document from the European Commission –A European Strategy for Data – calls the amount of data held by "Big Tech firms" a "major weakness" for Europe, and proposes several regulations to require sharing of data between public and private firms to create a "European data space." This document also proposes subsidizing European cloud providers while contemplating potential ex ante competition rules that would be applied against foreign firms.

It is important for the U.S. to engage with the EU on this issue to ensure that any proposals on sovereignty and European data do not include tools that would result in protectionism and discrimination against U.S. firms." (pg. 36-37) *(emphasis added)*

iii. Computer & Communication Industry Association: "The Commission is preparing extensive regulatory proposals (under the planned Digital Markets Act). In recent years, U.S. technology firms have seen a rise in protectionist actions relating to competition in the forms of antitrust enforcement and new regulations.

First, the EU has announced plans to impose new regulations on certain "structurally significant" digital businesses. This "ex ante" proposal is expected to be released in December 2020, and will restrict the competitive capabilities of large technology companies, making it harder to operate in European competitively. These regulations would largely apply to large U.S. platforms and exclude most European competitors.

According to media reports, these proposals will operate under the assumption that restoring "competitiveness" to Europe's digitally enabled markets requires outright prohibitions of certain types of conduct (e.g. so-called "self-preferencing"), structural separation obligations ("line of business restrictions"), and even opening up assets and infrastructure to less capable rivals (access obligations), helping European companies piggy-back off rivals' innovations and investments. In December, the Commission is expected to present its "Digital Markets Act" (a combination of both "ex ante" regulation and new digital market-only investigation and remedy powers, originally intended to apply horizontally as a "New Competition Tool", or NCT.

It is possible that other jurisdictions will follow the European approach to restricting the competitive threat of U.S. companies.

If implemented, these reforms would push competition law in a new direction towards a structural approach that favors smaller European competitors while ignoring the dynamic competition that takes place, the consumer welfare generated by the existing framework, and the innovation and investment incentives necessary to generate future technological breakthroughs. *(pg. 36-37) (emphasis added)*

iv. Information Technology Industry Council: "A new European Commission took office in May 2019 and has since pursued an active digital policy strategy under the banner of "technological sovereignty", which is geared towards boosting the capacity of Europe's domestic technology industry and may affect the conditions under which non-European firms can compete in the European single market. Under a new, sweeping Digital Services Act the EU is proposing new ex ante regulatory rules that may affect various aspects of U.S. platforms' business models. Other initiatives, described in more detail below, center on data governance, artificial intelligence, and cloud services. Maintaining and increasing the ability to develop key technologies and ensure their availability to the EU in the future is a legitimate goal, and ITI strongly supports the pursuit of these objectives in a manner that eschews protectionism and discrimination."

(pg. 18) (emphasis added)

v. ***National Foreign Trade Council:*** "Notably, since the European elections in 2019, EU leaders have actively promoted an aggressive, multi-pronged approach towards "technology sovereignty" as one of the two main policy objectives to be pursued by the current EU Commission. **Under this new policy umbrella, the EU is proposing new regulatory "ex ante" rules that would apply almost exclusively to U.S. platforms (under a new, sweeping Digital Services Act)**, as well as restrictions on cloud services, artificial intelligence and data. **EU officials have stated that the purpose of digital sovereignty is to create a "new empire" of European industrial powerhouses to resist American rivals. These unilateral regulations appear designed to discriminate against U.S. companies and to take aim at a slice of the $517 billion U.S. digital export market."** *(pg. 4-5) (emphasis added)*

d. Germany's GWB Digitization Act

i. ***Internet Association:*** **"Germany is reportedly considering allowing competition authorities to subject certain market-leading companies to prohibitions and penalties even if there has been no showing of anti-competitive abuse, which would be flatly inconsistent with U.S. and global practice.** The companies that would be targeted are online platforms and other companies that German authorities accuse of "transcending" their dominance in a given market because, for example, they are vertically integrated or control sensitive business data. Other proposed rules would also target online platforms, including a rule that would make it easier for competition authorities to oblige platforms to provide access to data. Many of these proposed rules include fuzzy definitions of longstanding concepts in competition law (such as "dominance" and "essential facilities") and depart from global competition norms, including by shifting the burden of proof away from competition authorities and towards targeted companies. Together these rules could stifle U.S.-German digital trade **and could serve as a model for other countries that are looking to challenge or undermine U.S. businesses operating in this sector.** *(pg. 53-54) (emphasis added)*

ii. ***Computer & Communications Industry Association:*** "Reports indicate that a central part of the reform will be to "move to a preventative level (ex ante) imposing precautionary antitrust responsibilities on companies rather than waiting for an abuse to take place before taking action." German authorities have also proposed targeting online platforms and other companies supposedly "transcend" their dominance in a given market based on vertical integration concerns or access to sensitive data. Another proposed rule would shift the burden of proof away from competition authorities and towards targeted companies. **Many of these proposals are starkly inconsistent with longstanding U.S. and global competition norms and, if adopted, could serve as trade barriers."** *(pg. 47) (emphasis added)*

II. Industry Submissions to the 2022 NTE

a. Korea's App Store Law

i. ***Information Technology Industry Council:*** "On August 31, 2021, the Korean Legislative Assembly's Legislation and Judicial Committee passed the "In-App Legislation," which bans large app store operators from requiring app developers to use their respective in-app payments systems. **The law appears to run contrary to Korean trade commitments by taking an approach that would disrupt standardized practices that ensure consumer privacy, security, and reliable access across markets, and with legislators' public statements effectively singling out two U.S.-headquartered companies.** The law will also restrict U.S. app developers' ability to reach the Korean market via trusted ecosystems." *(pg. 56) (emphasis added)*

ii. ***Coalition of Services Industries:*** "In August 2021, the Korean National Assembly passed legislation that requires mobile application marketplaces to permit users to make in-application purchases through payment platforms not controlled by the marketplace itself. **This legislation is global-first and bans a business model that is practiced by US mobile app marketplace providers, and not their Korean equivalents. It threatens a standard US business model that has allowed successful Korean content developers to reach global audiences, and is at tension with Korea's obligations under the Korea-US FTA.** In the absence of a payment service integrated into a mobile application marketplace, it is unclear how the application distributor could recover the costs it incurs in maintaining the mobile application marketplace, and monetize the broad benefits accorded to all application developers, including those from Korea." *(pg. 47-48) (emphasis added)*

iii. ***Computer & Communications Industry Association:*** "In August 2021, the Korean National Assembly passed legislation that requires mobile application marketplaces to permit users to make in-application purchases through payment platforms not controlled by the marketplace itself. **The scope of the law effectively creates a band on a predominately used U.S. model, at the exclusion of local equivalents. Further, policymakers supportive of the bill have made clear their intent to single out specific U.S. companies with the new law. The targeting of U.S. firms could conflict with Korea's trade commitments under the Korea-U.S. Free Trade Agreement, as well as commitments under Article XVII (National Treatment) of the WTO General Agreement on Trade in Services (GATS).** U.S. operators of application marketplaces are disincentivized to operate in a region where it is unclear how the application distributor could recover the costs it incurs in maintaining the mobile application marketplace." *(pg. 80-81) (emphasis added)*

iv. ***Internet Association:*** "In August 2021, the Korean National Assembly passed legislation that requires mobile application marketplaces to permit users to make in-application purchases through payment platforms not controlled by the marketplace itself. **This legislation is a global-first move that affected only two U.S. digital companies and none of their Korean competitors. It threatens a U.S. business model that has allowed successful Korean content developers to reach global audiences, and is at tension with Korea's obligations under the Korea-U.S. FTA.** In the absence of a payment service integrated into a mobile application marketplace, it is unclear how the application distributor could recover the costs it incurs in maintaining the mobile application marketplace, and monetize the broad benefits accorded to all application developers, including those from Korea." (pg. 83) ***(emphasis added)***

b. Australia's News Media Bargaining Code

i. ***Information Technology Industry Council:*** "The Code requires U.S. digital platform companies that display domestic Australian news content to create a contract for revenue sharing and notify news outlets of any changes to the company's internal algorithms. While companies have not yet been designated, the Code accords the Australian Treasurer unfettered discretionary power to designate companies to which the Code should apply. **As the Code would only affect U.S. companies, it appears to conflict with basic trade principles of national treatment and non-discrimination under the Australia-U.S. Free Trade Agreement (AUSFTA) and the WTO General Agreement on Trade in Services (GATS)."** *(pg. 18) (emphasis added)*

ii. ***Computer & Communications Industry Association:*** "Under the Code, designated platform services companies are required to engage in negotiations with Australian news publishers for online content. **Motivated by a desire to empower domestic news publishers,** the new rules would dictate that online services negotiate and pay Australian news publishers for online content, and disclose proprietary information related to private user data and algorithms.

(...)

Only two companies have been identified throughout deliberations. There are significant concerns from a procedural, competition, trade, and intellectual property perspective that USTR should pay close attention to. In particular, U.S. officials should monitor the implementation of the Code and its adherence to the principles of transparency, fairness and non- discrimination as consistent with the U.S.-Australia FTA." *(pg. 23-24) (emphasis added)*

iii. ***U.S. Council for International Business:*** "In February 2021, the Australian Government passed the News Media and Digital Platforms Mandatory Bargaining Code... To date, no platform has been designated, although the Code is subject to an annual review by the Treasurer commencing February 2022. In view of the impending Federal election and that news publishers are integral to the election, the process is politicized.

USTR should continue to pay close attention to the implementation of the Code and its adherence to the principles of transparency, fairness and non-discrimination as consistent with the U.S.-Australia FTA." *(pg. 6-7) (emphasis added)*

iv. ***Internet Association:*** "In February 2021, the Australian Government passed the News Media and Digital Platforms Mandatory Bargaining Code… To date, no platform has been designated, although the Code is subject to an annual review by the Treasurer commencing February 2022. In view of the impending Federal election and that news publishers are integral to the election; the process is politicized. **USTR should continue to play close attention to the implementation of the Code and its adherence to the principles of transparency, fairness and non-discrimination as consistent with the AUSFTA."** *(pg. 14) (emphasis added)*

c. EU's Digital Markets Act/Digital Services Act

i. ***Computer & Communications Industry Association:*** "Under the proposed text, companies that operate a "core platform service" must notify the European Commission upon meeting pre-defined thresholds for European turnover, market capitalization, and number of European consumer users and business users. **These thresholds have been set at levels where primarily U.S. technology companies will fall under scope, and some policymakers have proposed amending the thresholds to ensure that only U.S. firms fall under scope.** The list of "core platform services" furthermore carves out non-platform-based business models of large European rivals in media, communications, and advertising.

Once under the scope of the DMA, companies will be prohibited from engaging in a range of pro-competitive business practices (e.g., benefiting from integrative efficiencies). Furthermore, the Commission will be vested with gatekeeping authority over approval for future digital innovations, product integrations, and engineering designs of U.S. companies. The DMA would also in some cases compel the forced sharing of intellectual property, including firm-specific data and technical designs, with EU competitors, effectively requiring U.S. firms to subsidize rivals to promote competition. Unlike traditional competition enforcement, the Commission will be able to impose these interventions without an assessment of evidence, of any effects-based defenses, or of pro-competitive justifications put forth by the companies targeted." *(pg. 52) (emphasis added)*

ii. ***U.S. Council for International Business:*** "Since the European elections in 2019, EU leaders have actively promoted an aggressive, multi-pronged approach towards "technology sovereignty" as one of the two main policy objectives for the current EU Commission. Under this new policy umbrella, the EU is proposing new regulatory 'ex ante' rules that would apply almost exclusively to U.S. platforms (under the sweeping Digital Services Act and Digital Markets Act), as well as restrictions on cloud services, artificial intelligence and data. **EU officials have stated that the purpose of digital sovereignty is to create a "new empire" of European industrial powerhouses to resist American rivals. These unilateral**

regulations appear designed to discriminate against U.S. companies and to take aim at a slice of the $517 billion U.S. digital export market.

The recent years have already been marked by aggressive enforcement where U.S. tech companies have been subject to Europe's highest profile competition enforcement cases, often receiving record fines unheard of in the rest of the world. The European Commission has imposed record fines and essential facility-style rules on U.S. companies for conduct most other regulators and courts have found to be legal. The Commission has also required record repayments of tax revenues as part of its state aid cases.

(...)

The European Commission has proposed new legislation and enforcement tools for the digital marketplace ("Digital Markets Act"). **As the EU considers structural measures to address the digital marketplace, we urge USTR to work with the EU to ensure that it does not discriminate against U.S. companies through its laws and regulations, and that it upholds principles of non-discrimination, regulatory transparency, and technology neutrality in laws and regulations. It is important that regulatory approaches impacting digital services and technologies are developed in a deliberate and consultative manner subject to traditional trade principles, including non-discrimination, national treatment and most favored nation treatment.** In keeping with transatlantic regulatory principles, such regulatory frameworks must also include clear protections for due process and regulatory dialogue, as well as safeguards for IP, privacy, and security." *(pg. 59) (emphasis added)*

iii. ***Internet Association:*** "The European Commission published its Digital Markets Act (DMA) proposal in December 2020. **The DMA includes an array of extraordinary prohibitions that will apply exclusively to a small group of U.S. platforms. EU officials have been clear that they aim to use the DMA to reduce "dependence" on U.S. services and to support local industry, furthering the EU's current agenda of digital sovereignty.**

As proposed, the DMA would impose sweeping competitive restrictions on companies labeled as "gatekeepers," which the EU has defined narrowly to refer to a specific subset of U.S. technology providers, while excluding European digital rivals and other EU industries that compete with the U.S. technology sector. If enacted, US companies would be forced to comply with new obligations and regulatory restrictions that would damage their competitiveness with foreign firms, while the EU – as well as Russia, China, and other foreign rivals – would be entirely free of these restrictions.

Specifically, the DMA imposes a large number of restrictions on business activities that have previously been permissible under U.S. and EU law. Further, U.S. companies would have to meet a number of new requirements and restrictions under the DMA, including obligations to provide foreign rivals with access to proprietary and private information, ranking data, and internal tools; and restrictions on offering integrated services regardless of consumer welfare, security, and privacy considerations. For example, one of the most striking requirements under the DMA is an obligation for U.S. search engine providers

to "provide access, on fair, reasonable and non-discriminatory terms, to search ranking, query, click and view data to other providers of such services." This sort of obligation has no parallel in any other national law, and would present significant privacy, security, and intellectual property concerns to consumers and business users of search services, while appropriating highly valuable trade secrets from U.S. companies. The DMA's enforcement provisions would also lower the bar for EU officials to impose structural remedies on U.S. companies. In addition to potential fines of up to 10% of global turnover, the DMA includes a long list of potential sanctions, divestment requirements, structural separation requirements, and broader remedies for "systemic non-compliance." This framework gives the EU substantial new authority to potentially restructure the operations of U.S. companies.

... It appears that the EU's goal in circumventing competition norms is to lower evidentiary standards, shift burdens of proof, and eliminate opportunities to rebut findings—making it faster and simpler to issue crippling penalties and structural remedies on U.S. companies." *(pg. 35-36) (emphasis added)*

iv. ***Information Technology Industry Council:*** "In parallel, previous proposals have progressed through the legislative process. These include the bloc's new rules for online platforms in the Digital Services Act (DSA), the new Digital Markets Act (DMA), which sets out to address the challenges posed by "gatekeepers," and new rules for re-use of sensitive data held by the tech sector in the Data Governance Act (DGA).

ITI is closely involved in these legislative procedures and continues to underscore the need for the EU to pursue its policy objectives in a manner that eschews protectionism and discrimination.

» **The Digital Services Act** (DSA), published in December 2020, is aimed at harmonizing rules for the removal of illegal content online and rules related to the responsibility and liability of online platforms. It proposes new harmonized rules for flagging and taking down illegal content online, a verification mechanism for traders on online platforms, and the regulation of trusted flaggers (i.e., certified entities tasked with removing illegal content from platforms). The DSA also proposes differentiated obligations for what it identifies as very large online platforms, such as annual audits, data sharing with authorities and researchers, transparency of recommending systems, and risk management. The proposal is currently being amended by the Council of the EU and the European Parliament, with a final deal expected in 2022.

» **The Digital Markets Act** (DMA) is a draft law that targets large online platforms determined by Commission parameters to have a systemic role in the market. The DMA introduces obligations and prohibitions for companies that are designated as "gatekeepers" based on quantitative indicators related to revenue, number of users, and cross-border reach (across a minimum of three EU Member States). As drafted the Commission retains ample flexibility to perform a qualitative assessment and designate a firm as a gatekeeper regardless of the quantitative criteria. The DMA also gives the Commission far-reaching investigative powers over gatekeepers, including

the possibility to carry out on-site inspections, and practices perceived as having a distortive effect on competition. **Concerns remain that the DMA's application may be limited to a handful of primarily U.S.-headquartered firms.** The DMA is currently being amended in parallel by the Council of the EU and the European Parliament, with a final deal expected in 2022. **ITI encourages USTR and the U.S. administration to engage with the EU to ensure that the rules are targeted to proven and clear market failures and remain non-discriminatory in nature.** We also continue to advocate for the establishment of a regulatory dialogue in the context of the DMA to ensure that rules are fairly and transparently applied." *(pg. 28) (emphasis added)*

Coalition of Services Industries: "In December 2020 the European Commission issued the Digital Markets Act, a complex proposal that seeks to impose new restrictions on large online service providers, deemed "gatekeepers," in the name of promoting competition. **The scope of the law could impact U.S. companies disproportionately.**

... As the EU considers structural measures to address the digital marketplace, we encourage USTR to work with the EU to uphold principles of non-discrimination and technology neutrality in laws and regulations. It is important that regulatory approaches impacting digital services and technologies are not protectionist, but rather developed in a deliberate and consultative manner subject to traditional trade principles, including non-discrimination and national treatment. *(pg. 21) (emphasis added)*

vi. ***App Association:*** "The European Commission has already carried forward numerous regulations, directives, consultations, and proposals under the DSM that raise significant concerns for the App Association, including:

- **A range of competition-themed activities and policies focused on the EU's "digital sovereignty" that stand to cause damage to the digital economy and American small businesses' ability to operate in the EU.**[19]
- A proposal to regulate online platforms, via the Digital Markets Act, to address contractual clauses and trading practices in relationships between platforms and businesses. Additionally, there are attempts to regulate the free flow of information online through things such as the EU's Digital Services Act which centers around tackling illegal hate speech with the goal, moving forward, of removing illegal content from the internet.

[19] European Commission, The Digital Services Act package, available at https://ec.europa.eu/digital- single-market/en/digital-services-act-package." (pg. 12) *(emphasis added)*

d. Germany's GWB Digitization Act

i. ***Internet Association:*** "A new competition law entered into force in Germany in January 2021 that allows the German Federal Cartel Office ("FCO") to subject certain companies to prohibitions and penalties even if there has been no showing of an abuse of a dominant market position, which would be flatly inconsistent with U.S., EU and global practice. The companies targeted are online platforms and other companies that German authorities accuse of "transcending" their market power in a given market because, for example, they are vertically integrated or control sensitive business data. **After the new law became effective, the FCO immediately used its new powers and initiated investigations against US-based companies Facebook, Google, Amazon, and Apple alleging that these companies are of "paramount significance for competition across markets.**

Other rules in the new law also target online platforms, including a rule that makes it easier for competition authorities to oblige platforms to provide access to data. Many of the rules include fuzzy definitions of longstanding concepts in competition law (such as "essential facilities") and depart from global competition norms, including by shifting the burden of proof away from the FCO and towards targeted companies. **Together these rules come close to introducing a sector-specific regulation of online platforms by means of antitrust law and could serve as a model for other countries worldwide that are looking to challenge or undermine U.S. businesses operating in this sector.** Overall, the new regime is likely to negatively affect U.S.-German digital trade." *(pg. 52) (emphasis added)*

ii. ***Computer & Communications Industry Association:*** "Germany recently reformed its competition rules, with a new law effective January 19, 2021. The rules were amended to de-emphasize causality requirements and the Federal Cartel Office (FCO) was provided with completely new enforcement instruments, especially for digital platforms, providing much lower intervention thresholds and limiting possibilities for judicial review.

(...)

Many of these rules are starkly inconsistent with longstanding U.S. and global competition norms and effectively serve as trade barriers. Most importantly, the new competition rules were written to be enforced solely against U.S. companies. Current investigations under this new regime are limited to U.S. tech companies." *(pg. 63-64) (emphasis added)*

Source Code

A Trade-Related Barrier to the Right to Repair

(A Transatlantic Study)

Anthony D Rosborough*

17 October 2025

Report commissioned by TACD, the Transatlantic Consumer Dialogue. Research for this report was made possible with the support of the Heinrich-Böll-Stiftung European Union | Global Dialogue & Heinrich-Böll-Stiftung Washington, DC USA | Canada | Global Dialogue

Table of Contents

Executive Summary

In recent years, conflicts between software access restrictions and Right to Repair (R2R) legislation has become a growing concern for policymakers and repair advocates around the world. Consumers have come to increasingly depend on electronic devices that integrate sophisticated hardware and embedded software. When those devices break or require maintenance, owners often lack the software or software-based tools required to fix them. In some cases where replacement parts and information may be readily available, device software and software-integrated tools present a barrier to independent repair. In response, legislators in both the United States and the European Union have been enacting R2R laws designed to empower consumers and professional repairers with access to these resources to foster a circular economy and reduce electronics waste.

At the same time, trade negotiators on both sides of the Atlantic have been concluding free trade agreements (FTAs) that include digital trade provisions that protect software source code and algorithms from inspection and disclosure by governments or access by third parties. These provisions, such as those found in the *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (CPTPP), the *US-Mexico-Canada Agreement* (USMCA) and subsequent EU-led agreements, bar governments from requiring device manufacturers to transfer or disclose source code or algorithms as a condition for market access.[1]

Though to date these parallel policy developments have (for the most part) occurred in isolation from one another, this report examines their potential for interaction and future conflict as contemporary FTAs and R2R mandates with software disclosure obligations come into effect. These seemingly distinct legal and policy developments may come into conflict where, for example, R2R mandates explicitly or implicitly require manufacturers to transfer or provide access to source code or algorithms for the benefit of third-party repairers or consumers.

Drawing from statutory texts, recent trade agreements, policy briefs, and media reports, the study assesses the importance of access to software tools for repair, analyses domestic R2R legislation in the United States and Europe, surveys source-code provisions in major agreements, evaluates potential conflicts, and offers recommendations for policy makers. The report's key findings are that:

1. **Repair now depends on software.** Parts pairing, diagnostic software, firmware[2] updates, and calibration tools are now essential repair resources. Both EU and U.S. R2R frameworks explicitly recognise that access to these software-based tools is as critical as access to parts and manuals. Recent EU legislation[3] and some U.S. state laws (New York, Minnesota, Colorado) impose obligations on manufacturers to provide repair-related software to third parties. In Europe this

includes the Directive on common rules promoting the repair of goods ("R2R Directive")[4], the EcoDesign for Sustainable Products Regulation ("ESPR")[5], and the EcoDesign Regulation for Smartphones and Tablets ("ERST")[6]. U.S. state-level R2R laws include those passed in New York[7], Minnesota[8], and Colorado[9]. These obligations stop short of requiring explicit access to source code, but they cover keys and utilities that could be *legally construed* as such.

2. **FTA source code secrecy provisions create friction.** Agreements like USMCA, CPTPP, and EU-Japan EPA prohibit governments from requiring access to source code (and in some cases algorithms). Depending on their interpretation, manufacturers may invoke these clauses to resist obligations under R2R laws that require provision of software tools or firmware to third parties, even if those obligations target primarily object code or binaries.

3. **Treaty language diverges in restrictiveness.** Agreements like the USMCA adopt broad protections for source code and algorithms with only narrow, case-by-case exemptions, whereas newer EU-led agreements provide more permissive exceptions for regulatory oversight and public policy objectives. This variation creates uncertainty for R2R enforcement and potential conflicts.

4. **Shifting policy positions present an opportunity for change.** In late 2023, the U.S. reversed its prior stance on digital trade and source code secrecy rules at the WTO, citing the need to preserve domestic regulatory space (including the R2R). The EU's digital trade agenda continues to advance source code secrecy rules but with increasingly explicit exceptions and public-interest acknowledgements. This indicates a possible convergence around a more balanced approach that accommodates both digital trade and R2R objectives, signalling an opportunity to revisit these rules and their impacts.

1. Introduction

1.1 Context and Background

Demands for greater product repairability and durability can be traced back many decades[10], but the modern R2R movement's genesis is situated in the early 2000s, stemming largely from within the automotive sector.[11] The movement has since expanded widely into the realms of consumer electronics, home appliances, commercial and industrial equipment[12], and even critical infrastructure.[13] In essence, R2R advocates argue that consumers and independent repair technicians should have reasonable access to the parts, tools, and information needed to fix the products that they own. Proponents highlight environmental benefits (reduced waste and carbon emissions), economic advantages (lower repair costs and increased market competition), and social benefits through the diffusion of technical knowledge and information sharing. In the EU, the United States, and beyond, R2R advocates have found enormous success in passing law and policy that helps achieve these goals in various ways.

Key to this success has been the movement's open and flexible norm in pushing for a *right* to repair. This permits several complementary policy approaches that fall under the movement's umbrella. In broad terms, these approaches can be placed into two broad categories of *negative rights* and *positive rights*.[14] The negative right approach involves reducing legal and regulatory barriers to independent and self-repair. This results in a focus on establishing new exceptions and limitations to various intellectual property rights, preventing manufacturers from voiding warranties following independent repairs, and emboldening market competition or anti-trust authorities with greater enforcement mechanisms. In essence, the negative rights approach to the R2R is motivated by the pursuit of various individual and consumer *freedoms*.

The positive right approach, on the other hand, involves imposing new obligations on manufacturers to provide consumers and independent repairers with the necessary parts, tools, and information to complete repairs at a reasonable cost. In this way, it is focused primarily on securing various *entitlements*. This ordinarily involves amendments to consumer laws and the establishment of new and bespoke enforcement and compliance mechanisms to ensure that manufacturers follow prescriptive requirements as to the design of products and their support for consumers after sale.

Importantly, positive rights approaches to the R2R ordinarily impose ongoing obligations to provide replacement parts, information, and tools (including software) to consumers after the point of sale. Though R2R schemes in the EU and across United States differ in some respects, they commonly share these aspects of a positive rights approach, including mandated access to diagnostic software, firmware, and software-based tools in relation to various devices and products.

1.2 The Essential Role of Software for the Right to Repair

The increasing focus on software and software-based tools for repair practices is in response to the widespread computerisation and software-dependency of products and devices. Both the EU and United States' recent R2R policy developments have drawn attention to these dynamics. In late 2023, for example, the European Parliament approved a set of measures banning "parts pairing", a software-based product design practice where a device's components are digitally linked to its serial number, preventing third-party or self-repair (even with genuine parts).[15] State-level R2R bills in the United States in recent years have also shown an emphasis on forcing manufacturers to provide access to embedded software and the means to 'reset electronic security locks'.[16]

The R2R movement's emphasis on software disclosure obligations has been (unsurprisingly) met with pushback from manufacturers. This is largely due to the crucial role that software and software-based product controls play in protecting business models and exclusive supply chains. In legislative debates, hearings, and public pronouncements relating to the R2R, manufacturers have often opposed disclosure of software-tools in particular[17], countering that restricting access is necessary to prevent intellectual property infringement, tampering with products, or ensuring public safety or compliance with other regulatory requirements.[18] In a few instances, manufacturers have sought to resist, narrow, or find alternative pathways to mandated disclosure or access to their software and software-based tools, whether through litigation or voluntary agreements with independent repairers on manufacturers' terms.[19]

1.3 Growing Friction with International Trade

Against this backdrop, the international trade realm has been gradually introducing a new potential constraint on mandated disclosure and access to software as part of R2R policy. Over the last decade, a "no-forced disclosure" template for software has spread through FTAs' "digital trade" chapters. These sections, typically titled "source code", prohibit governments from requiring access to, or transfer of, source code and increasingly "algorithms" (often ambiguously defined). In some cases, this prohibition is narrowed to situations where transfer or access is required for market entry, while in older EU agreements the prohibition is general and potentially more expansive. These new rules are often subject to only narrow case-by-case exceptions that do not envision comprehensive and perpetual regulatory frameworks like the R2R.

Though this special source code protection in FTAs was orchestrated to protect trade secrets and cybersecurity amidst geopolitical rivalry and tensions, the net effect is to elevate software secrecy from a matter of domestic private law into an international commitment. Even where R2R frameworks may have strong public-interest dimensions, the presence of these new rules may provide well-resourced firms with a new avenue, forum, and vocabulary to resist or narrow R2R mandates that oblige provision of software and software-based tools. And though R2R frameworks may not explicitly require

disclosure of human-readable source code, manufacturers may nevertheless argue that compelled provision of tools, programs, firmware, or keys exposes protected logic or amounts to a *de facto* disclosure of algorithms.

There is a tension at play in that R2R mandates treat software as a necessary instrument of product maintenance and consumer choice, while contemporary FTAs treat software as a sensitive asset to national security that must be insulated from mandatory disclosure to third parties. As the EU and the United States move from high-level principles to more concrete and enforceable duties on software tools and anti-pairing measures, friction with FTA source code protection clauses is inevitable. That friction will be felt most acutely in sectors where embedded software governs core device functions with potential safety implications if accessible by third parties. Friction will also be felt where manufacturers rely on proprietary software ecosystems to deliberately prevent third-party repair and servicing of their products and devices and protect exclusive business models.

1.4 Report Roadmap

The purpose of this report is to identify the areas of potential tension between domestic R2R frameworks and emerging FTA source code protections. This includes offering recommendations to chart a successful path forward for R2R policy and recalibration of overbroad trade rules on both sides of the Atlantic. Accordingly, Section 2 lays out the practical role of software in repair activities, showing its role in calibration of devices following physical repair, diagnostic scans and reading fault codes, and firmware updates. Section 3 then analyses a selection of recent R2R policy developments in the EU and United States that show a strong emphasis on software and software-based tools, including U.S. state-level bills covering consumer electronics and the EU's R2R Directive and the ESPR. Section 4 explains the origins and history of FTA source code protections before examining a selection of treaty language from recently concluded agreements to exemplify the overall trend and approach. Section 5 then explores the potential areas of conflict and tension between FTA source code protections at the international trade level and domestic R2R frameworks in the United States and EU. Finally, Section 6 concludes with a series of conclusions and recommendations for policymakers and trade representatives.

2. The Practical Role of Software in Repair Activities

Modern electronically enabled devices and products are increasingly software-dependent, and this fundamentally changes the landscape of repair and maintenance. In the past, repairing a device might have involved simply swapping purely mechanical parts or soldering components, with minimal need for supplementary software or

software-enabled tools. Today, however, everything from smartphones and laptops to cars, farm tractors, and even medical devices contain embedded computers and software. This radically changes repair practices, the knowledge and skills required to carry them out, and the tools and resources needed to complete them properly.

This trend is part and parcel of the proliferation of "ubiquitous computing", a design paradigm where computing appears seamlessly anytime and everywhere, embedded into a wide range of devices and products through smaller and more energy efficient hardware.[20] Ubiquitous computing is closely related to the broader Internet-of-Things (IoT) concept. This refers to a network of physical objects ("things") with embedded computer hardware, sensors, and other technologies that exchange data with other devices and systems over the internet or other communications networks.[21]

At the end of 2024, there were approximately 18.8 billion connected IoT devices globally, marking a 13% increase from the year prior. Projections indicate that this number will more than double (reaching over 40 billion) by the year 2030.[22] Beyond these facts and figures however, the growth of software-dependent devices can be observed in more anecdotal terms. Seemingly every product – from toothbrushes to home appliances – is now packaged with "smart" or connected features of one kind or another. These technological shifts mean that fixing a hardware problem frequently requires access to software, firmware, or digital keys that are often only made available through the manufacturer's supply chain or network. Across a wide range of product categories, consumers and independent technicians frequently find that software and software-based tools are as critical as screwdrivers in a repair toolkit.[23]

The following sections break down several key categories in which software, firmware, and software-enabled tools play a pivotal role in repairing and maintaining a variety of electronic devices. These are broken down into categories that share considerable overlap but generally fall along the lines of replacing physical parts, diagnosing errors and faults, and calibrating or fine-tuning equipment following repairs. For each category, product examples are provided to illustrate how software bottlenecking manifests in both consumer electronics repair and other technologies (with parallels in both the EU and United States contexts).

2.1 Parts-Pairing and Software Locks

Parts-pairing refers to the practice of electronically linking a replaceable component to the device via onboard software, so that the device will recognise only an 'authorised' part. In practical terms, manufacturers embed microchips or serial numbers in components and program the device's firmware to verify those identifiers. If a part's ID does not match the device's expected identifier (for example, because the user installs a replacement part from another device), the onboard software may refuse to fully operate or may disable certain functions without authorisation by official software.

This approach to device and component design should be familiar to owners of consumer grade printers, which often have systems to detect whether replacement ink cartridges are 'authentic'. Parts-pairing refers to a broader and more robust implementation of this system design approach to encapsulate many of a device's physical components, rendering many repairs dependent on specialised software that is not ordinarily made available to end-consumers. This tends to undermine self-repair and independent shops and refurbishers by presenting error messages or lost features following successful physical repairs.

2.1.1. Parts-Pairing in Apple's Smartphones

Likely the most well-known (and widely reported) example of parts-pairing is in relation to Apple's line of smartphones. iPhones manufactured in recent years have multiple serialised components (screens, batteries, cameras, Touch ID/Face ID sensors). If, for example, a consumer or unauthorised repairer attempts to replace a broken iPhone display or a worn-out battery, the phone's onboard software will detect the new part's serial mismatch. As a result, certain features will stop working and warning messages will appear. For instance, the ambient light auto-adjust feature (known as "True Tone") is disabled after a screen swap, and the system will persistently warn that it 'cannot verify' a non-genuine display or battery.[24] Even more critically, an authorised swap of an iPhone's Touch ID or Face ID module may outright break those biometric login features for security reasons.

The consequence of these parts-pairing techniques is that only Apple (or an Apple-authorised technician) has the software tools to reset parts-pairing by resetting the serial numbers of replacement parts. The tight grip kept on these software tools by Apple has caused independent repair shops to lose business, as customers understandably are less interested in repairs that result in degraded functionality or incessant 'genuine part' warnings after repair.[25] As a result, many R2R advocates have flagged Apple's parts-pairing design and unwillingness to share software tools as a deliberate strategy to monopolise repairs.

Following increasing pressure on lawmakers by R2R advocates to ban these practices through legislation, Apple only recently announced a new on-device "Parts & Repair Assistant" application that will allow owners of iOS 18 and newer iPhones to pair used genuine parts (from donor devices) for certain iPhone models without specialised equipment.[26] While an important step for the R2R, parts-pairing practices are still widely used by Apple outside of its line of smartphones, highlighting the enduring and crucial role of external software tools to complete physical repairs.

2.1.2. Game Consoles and the Automotive Industry

Parts-pairing is also prevalent across a broader range of consumer electronics, including game consoles. A notable case of this is the Microsoft Xbox One. To combat game piracy and hardware tampering, Microsoft digitally paired each console's optical

disc drive to its motherboard at the factory. The console's firmware checks that the installed DVD/Blu-ray drive is the original upon each startup. If it is not, the console will refuse to play the game or media.[27] As Microsoft itself has explained, "If your Xbox One optical disk drive broke, you can't take someone else's optical disk drive and plug it in. It won't work. These two things have to be paired together and only our factories can pair them."[28] The effect of this a significant impediment to independent repair, with one of the most failure-prone components (the disc reader) may render the entire device inoperable if it fails and the manufacturer's software tools are not made available.

The automotive industry has also begun to wrestle with the increasing prevalence of "VIN locking", a type of parts-pairing that presents barriers for independent automotive mechanics.[29] Despite the long history of modularity and interoperability in the automotive industry, VIN locking now enables manufacturers to digitally lock specific parts and components to a single vehicle.[30] This has become more prevalent with the rise of electric vehicles (EVs) which feature more robust layers of computerisation than their internal combustion predecessors. For independent automotive technicians, completing many physical repairs and parts replacements on modern vehicles requires access to the manufacturer's bespoke diagnostic tools and reprogramming protocols, which are often costly or difficult to obtain for smaller shops.

Cumulatively, these examples show that in modern devices the "tool" that makes physical parts replacement possible is supplementary software or keys/codes required to access and modify existing on-board software. Manufacturers serialise components and bind them (via firmware checks, cryptographic handshakes, or digital keys) to a specific device that replacements trigger warnings or lose functionality. In the end this means that completing a repair successfully typically requires access to software utilities in addition to analog tools and parts.

2.2 Diagnostic Software and Scan Tools

While parts-pairing reveals the importance of software for modifying physical components of devices, the role of diagnostic software and scan tools reveals the importance of software for understanding faults requiring repair at the outset. Many of today's devices and products are designed to detect faults and log error codes through onboard software. When something goes wrong (be it a sensor failure, a motor issue in an appliance, or a malfunctioning circuit), the device's firmware may force the device into a reduced functionality state (sometimes referred to as "safe mode" or "limp mode") and/or display error messages. Reading, understanding, and clearing these errors to restore full functionality are tasks that all commonly involve additional software tools or special keys or codes. As one might imagine, these types of diagnostic tools or codes are often not made widely available to consumers or independent repairers.

2.2.1 Taylor C602 Soft-Serve Machine (McDonald's Restaurants)

The Taylor C602 soft-serve ice cream machine (a standard in most McDonald's restaurants around the world) is a highly publicised example of how decisive software access is in diagnosing faults. The C602 periodically runs a complex thermal and pasteurization cycle for sanitisation purposes that frequently (and notoriously[31]) results in equipment failure.[32] Putting these ice cream machines back into operation requires navigating service menus, entering program codes known only by the manufacturer, as well as clearing specific error codes before the unit can operate properly again.

Crucially, much of these capabilities are kept secret or hidden from users and McDonald's franchisees. These capabilities are also undocumented in publicly available user manuals and require special tools to access them, leaving Taylor with a *de facto* monopoly on repair and servicing.[33] The prevalence and global reach of this issue resulted in a technology startup Kytch producing a device that attaches to the internal control of the C602 to decode error messages and reroute diagnostic data over the internet to restaurant managers and operators, enabling better detection of issues and troubleshooting.[34] Development of this device later resulted in legal battles between Taylor, Kytch, McDonald's, and its franchisees, resulting in Taylor producing and selling its own version of the device.[35]

Overall, the C602 serves as a helpful example of the contention that diagnosis and understanding faults in computerised devices and equipment often requires special access to software logs, error codes, and hidden menus. This access is facilitated either through supplementary software, or special keys or codes to access and modify software already present on the device. Absent access to these resources, device owners and even skilled technicians are forced to deal exclusively with manufacturers' networks for repair and servicing.

2.2.2 "Tesla Toolbox" Diagnostic Software

Diagnostic tools have a lengthy history in the automotive industry, and over the last several decades the industry has settled on common formats and data protocols to provide vehicle owners and independent technicians with crucial repair information.[36] Despite this standardisation, however, many manufacturers have begun to implement more sophisticated and bespoke systems for diagnosing faults.[37] A cutting edge example of proprietary diagnostic software is Tesla's "Toolbox" platform. The network-connected diagnostic software communicates with the car's onboard computer for deep diagnostics, understanding faults, and to run tasks like controller resets and programming new components. Tesla originally withheld access to Toolbox for consumers and independent technicians entirely, leaving salvaged or modified Teslas often crippled or with reduced functionality. Following increased pressure from lawmakers and repair advocates, however, the manufacturer began offering paid access to the platform in 2021. Toolbox access is facilitated through a service subscription

program with two tiers: one giving access to repair manuals and parts catalogs, and a higher tier unlocking diagnostics.[38] Tesla's Toolbox platform underscores how control over software tools can limit (in absolute fashion) the ability for consumers and independent technicians to diagnose faults and give effect to physical repairs.

2.3 Calibration and Configuration

Closely related to parts-pairing, authenticating replacement parts, and diagnosing errors or faults, software also plays a key role in calibration or fine tuning of devices following successful physical repairs. Calibration processes like aligning a camera module or configuring a new battery's charging parameters are often the final step in a repair process.

2.3.1 Apple's "Service Toolkit 2" Calibration Software for iPhones

In addition to software needed to successfully pair replacement parts, modern smartphones also require software utilities for successful calibration and configuration. This is especially true for higher-end devices like Apple's iPhone. Apple historically used an internal iPhone calibration machine (known as the "Horizon Machine") to recalibrate components like the Touch ID fingerprint sensor after screen repairs.[39] Today, however, most calibration tasks on iPhones is carried out through software-only tools like Apple Service Toolkit 2 ("AST 2").[40] This is a cloud-based diagnostic platform and system configuration tool that finalises repairs. These tools perform tasks like True Tone display recalibration, battery health resets, and facilitate parts-pairing for replaced components.

In 2023, following increased pressure from pending R2R legislation, Apple released a tool to consumers as part of its "Self Service Repair" program with similar functionalities to AST 2. This allows users to initiate cloud calibration processes post-repair.[41] This iOS-based application, "Repair Assistant", downloads the necessary firmware/calibration data for components like screens, batteries, or Face ID modules.

It should be pointed out that Apple is not the only manufacturer to rely on specialised software tools for calibration of this sort. Other smartphone and laptop makers also use proprietary software (though often less publicised and well-known). Many Android manufacturers have internal diagnostics or firmware flash tools for their repair centres.[42] The technical roles are similar in that calibrating sensors, updating firmware, and clearing error codes often requires access to specialised software utilities. But Apple's calibration tool exemplifies the increasing sophistication of software-based utilities that are required as part of many repair processes, requiring active connection to the internet and an authorised account.

2.3.2. GE's "Smart HQ" Service Calibration Tool

GE's Smart HQ Service is a subscription diagnostic platform only made available for 'professional' technicians. It is used with a GE Bluetooth module that plugs into an appliance's service port jack and pairs with an enabled phone or tablet application.[43]

Once connected, the app can read log data, calibrate components, and install firmware updates. GE sells the hardware module separately and charges an ongoing subscription for access to the software and cloud features.[44]

Smart HQ enables post-repair configuration and calibration that is increasingly essential to restore full functionality after physical repairs. GE's own training webinar materials highlight being able to "enter service mode" and "run calibration routines" along with targeted tests of fans, heaters, and sensors.[45] In refrigerators, industry reporting has described cases where replacing an ice maker or other component requires reprogramming and calibrating tolerances via Smart HQ. As of 2025, GE has advertised a subscription to the Smart HQ service at $600.00 per year (USD) in addition to a $199.00 (USD) Bluetooth service module.

The Smart HQ service illustrates how modern repair practices frequently involve software-based diagnostic tools for component actuation and calibration routines. Without this software layer, technicians may leave physically repaired devices out of spec. Though GE markets these tools as ways to reduce misdiagnosis and accuracy of repair, it is indicative of a broader trend of relying on software tools to gatekeep access to repair, limiting participation to professional repairers or those willing to invest in commercial grade subscriptions to software platforms.[46]

In sum, the foregoing examples underline the notion that repairing modern products and devices using only analog or physical tools is increasingly becoming a thing of the past. The decisive tool in many situations is often a software-layer, whether through accessing on-board software using special keys or codes or with software-enabled supplementary tools. These can be required in either identifying fault states, authenticating replacement parts as 'genuine', or calibration routines as the final step.

3. Right to Repair Mandates Requiring Access to Software

Given the crucial and instrumental role of software tools in repair practices, it should come as no surprise that access to these resources forms a key component of R2R legislative frameworks in both the United States and the EU. The following sections survey a selection of recent R2R policy developments in both jurisdictions that impose obligations on manufacturers to provide software tools.

3.1 The European Union's R2R Framework

To provide a brief introduction to lawmaking in the EU, its legislative institutions operate under the principal of conferral. This means that it may only act within the competencies stipulated by its constating treaties. The two primary legislative instruments created by EU institutions are "Regulations" and "Directives". The former has

general application and are binding in their entirety, making them directly applicable in all EU member states. Directives, on the other hand, are binding as to the result to be achieved, leaving member states the choice of form and methods and requiring transposition into national law by a prescribed deadline.

In practice, Regulations are used for uniform and immediately operative rules, while Directives set common objectives and minimum standards that national legislatures must implement. A core legislative competency of EU institutions is a focus on internal single market harmonisation and product standardisation.[47] As is described further below, this legislative focus helps lay the groundwork for a robust and prescriptive R2R framework in the EU, including mandated access to software and software-based tools.

The EU has embarked on a broad and ambitious R2R agenda as part of its sustainability and circular economy goals. Launched under the European Green Deal in 2019 and the Circular Economy Action Plan (CEAP) in 2020, this agenda aims to extend product lifespans, reduce e-waste, and empower consumers and independent technicians to repair products rather than replace them. A key focus of the EU's R2R policy has been in ensuring access to the parts, information, and software-based tools needed for repair.

Over the past five or so years, the EU has introduced a comprehensive suite of laws and policies that contribute to its R2R framework, including a mixture of high-level strategic initiatives that provide direction, new legislation on product design, and consumer protection laws to promote repair and transparency:

3.1.1. Ecodesign for Sustainable Products Regulation (ESPR)

The ESPR[48] creates a framework for setting product design and performance requirements and supersedes the older (2009) Ecodesign Directive.[49] It entered into force on 18 July 2024 and empowers the European Commission to adopt delegated acts imposing specific sustainability and circularity requirements on nearly all categories of physical goods, including software-dependent devices. These requirements cover aspects like durability, repairability, and recyclability and information disclosure at the time of sale. Crucially, the ESPR mandates the development of Digital Product Passports (DPP) for certain products. These are digital records that provide standardised information on a product's composition and repairability (including the availability of spare parts, software tools, and instructions) to consumers, repairers and other stakeholders.

The ESPR can be best understood as setting the EU's "design for repair" agenda, ensuring new products are engineered with repair in mind and that information and resources (including software) is accessible via DPPs. Though the ESPR does not directly mandate disclosure or access to software necessary for repairs, Annex I of the proposal lists parameters to improve repair and maintenance, including "conditions for access or

use of required hardware and software" needed to repair products.[50] Furthermore, future Ecodesign implementing rules may also require manufacturers to supply any specialised software or digital tools necessary to repair products.

3.1.2. The EU R2R Directive

Entering into force on 30 July 2024, the R2R Directive creates a unified EU framework to strengthen consumer rights and obligations of manufacturers. In contrast to the ESPR's focus on pre-market repairability by design, the R2R Directive sets the conditions for repair after a product has been purchased by a consumer. The aim of the R2R Directive is to make repair a more attractive and accessible option throughout the product's useful life. It amends a number of existing legal instruments (such as the Sale of Goods Directive) to establish a suite of new standardised obligations on manufacturers of certain product types. The deadline for EU member states to implement the R2R Directive is 31 July 2026.

Touching upon software tools specifically, the R2R Directive's Annex II provides a list of product categories for which manufacturers must provide parts and "tools" needed for repair at a "reasonable price".[51] In this context, "tools" are defined broadly to encompass not only physical tools, but also repair-related software tools, firmware, diagnostics, or similar auxiliary means needed to carry out repairs properly. Recital 18 of the Directive clarifies that:

> "…[M]anufacturers are to provide access to spare parts, repair and maintenance information or **any repair related software tools, firmware or similar auxiliary means**."

This general principle is reflected at Article 5(6) of the R2R Directive, which sets out the general obligations on manufacturers to facilitate the R2R for certain goods and products[52], including that:

> "Manufacturers shall not use any contractual clauses, **hardware or software techniques that impede the repair of goods**…unless justified by legitimate and objective factors including the protection of intellectual property rights…"

Put together, these obligations imply that, where manufacturers of pre-existing software-dependent devices have invoked techniques that necessitate software tools for effective repair, they must now provide access to those tools and utilities as part of their obligations under the Directive. Looking ahead, this also means that device manufacturers may not employ software restrictions or keys on future products purely to block independent repairs.

3.1.3. EcoDesign Regulation for Smartphones and Tablets (ERST)

Acting parallel to the ESPR, the EU enacted the ERST[53] in 2023 under the old 2009 EcoDesign Directive. These rules came into effect on 20 June 2025 and are intended to

ensure that mobile phones and tablets (in particular) sold in the EU are repairable. The ERST imposes a number of new and detailed obligations on device manufacturers in relation to software and software tools, including that manufacturers supply firmware, diagnostic software, or digital keys needed in repair activities. These are the first binding set of prescriptive and detailed rules creating the R2R smartphones and tablets in Europe.

The ERST implicitly distinguishes between manufacturers' obligations to release operating system updates and software tools needed for "serialised parts", or parts that are subject to parts-pairing techniques. 'Serialised parts' are defined as:

> "…a part which has a unique code that is paired to an individual unit of a device and whose replacement by a spare part requires the pairing of that spare part to the device by means of a software code to ensure full functionality of the spare part and the device".

In the case of smartphones, for example, the ERST repeats language found in the R2R Directive by requiring manufacturers to:

> "…provide non-discriminatory access for professional repairers and end-users to any **software tools, firmware or similar auxiliary means** needed to ensure the full functionality of those spare parts and of the device in which spare parts are installed during and after the replacement…"

Being enacted pursuant to the 2009 EcoDesign Directive, an important feature of the ERST is that EU member states are empowered to "designate authorities responsible for market surveillance" to ensure compliance with these requirements. This entitles regulatory authorities at the member state level to:

> "…organise appropriate checks on product compliance…and oblige the manufacturer or its authorised representative to recall non-compliant products from the market…[and] require the parties concerned to provide all necessary information, as specified in the implementing measures [and] take **samples of products and subject them to compliance checks.**"

Member states could therefore launch compliance investigations under the ERST that require device manufacturers to provide access to various software tools and firmware, as well as engage in reverse engineering investigations to determine regulatory compliance. As is discussed further in Part 4 below, this has important implications for FTA source code protections in some recent trade agreements.

Each of the above policy frameworks contributes to the EU's increasingly comprehensive policy architecture for the R2R. The ESPR (and product-specific regulations pursuant to it) address the supply side of product design and produce obligations to supply parts, software, and information. The R2R Directive, on the other

hand, address the demand side, including emboldened consumer rights, transparency, and fostering aftermarket repair services. These measures mutually reinforce one another to create a layered approach to the R2R throughout the EU.

3.2 R2R Legislation in the United States

In contrast to the EU's more centralised approach, the United States has seen R2R initiatives emerge primarily at the state level. To date, there is no federal R2R statute, though a proposed "Fair Repair Act" was introduced and discussed in Congress in 2021-2022 but never passed.[54] Nevertheless, advocacy continues in Washington, and federal agencies like the Federal Trade Commission (FTC) have shown interest in addressing restrictive repair practices through anti-trust enforcement.[55] In the meantime, state legislatures have led the charge, being primarily responsible for consumer law. As of early 2025, lawmakers in all 50 states have introduced or passed some form of R2R legislation.[56]

Being legislated at the state level, these statutes only regulate conduct occurring within the territory of those states which have enacted them, such as the sale or service of goods to residents in that state. This means that a resident of a state without R2R legislation cannot "import" another state's R2R protections simply by travelling there or owning a product sold in a state with R2R legislation in effect. Despite their territorial limitations in this regard, state-level R2R bills in the United States have made enormous progress in creating new obligations on manufacturers to provide parts, tools, information, and software to support independent and self-repair. Below is an analysis of a subset of these state level R2R laws that emphasise the provision of access to software or software-enabled tools as an illustration of the U.S. approach.

3.2.1 New York's Digital Fair Repair Act (2023)

New York was the first U.S. state to pass a broad-based consumer electronics R2R law. The *Digital Fair Repair Act*, which came into force in late 2023, requires electronics manufacturers to make available to owners and independent repair providers "the parts, tools, and documentation" for most devices first manufactured or sold in New York.[57] In practice, this means that original equipment manufacturers (OEMs) must provide (either directly or through authorised repair partners) documentation, parts, and tools.

The underlying 'fairness' principle that shapes the bill is that manufacturers must provide these resources to independent and third-party technicians on the same terms that their own 'authorised' service providers receive them. Importantly, the New York bill explicitly defines "tools" to include:

> "…**any software program, hardware implement, or other apparatus** used for diagnosis, maintenance, or repair…including software or other mechanisms, that provide, program, pair a part, calibrate functionality, or perform any other function required to repair or

> update the original equipment or part back to fully functional condition…"

While New York's Act establishes quite broad obligations in this regard, it also contains an important limitation to protect intellectual property, making clear that nothing in the bill requires a manufacturer to "divulge any trade secret or licence any intellectual property".

In terms of practical scope, New York's Fair Repair Act covers "digital electronic equipment", which is broadly defined as any product that depends on embedded digital electronics to function. At the same time, the bill also excludes many categories of equipment, including motor vehicles, off-road equipment, medical devices, home appliances, gaming consoles, and certain industrial and commercial equipment. The effect is that New York's law is limited to consumer-grade electronics, smartphones, and similar personal devices, while at the same time imposing quite broad and far-reaching obligations on manufacturers of those products. In spite of these important carve-outs, New York's *Digital Fair Repair Act* is generally viewed among R2R advocates as a landmark in requiring manufacture to share both physical and software-based tools needed for independent repairs.

3.2.2. Minnesota's Digital Fair Repair Act (2024)

Following New York's lead, Minnesota began charting a path toward its own *Digital Fair Repair Act* in 2023, coming into effect on 1 July 2024.[58] This bill is considered one of the broadest state-level R2R bills to date, covering a wide range of electronic products that fall under the umbrella of "digital electronic equipment". This is defined as:

> "…any hardware product that depends, in whole or in part, on digital electronics embedded in or attached to the product in order for the product to function…"

Similar to the New York bill, however, Minnesota's act exempts certain products and devices, including motor vehicles, medical devices, video game consoles, and off-road heavy equipment.[59] Despite these exclusions, Minnesota's law essentially covers everything else in the consumers and business electronics realm.[60] One consequence of this expansive approach (contrasting from New York's bill) is that the Minnesota bill applies to home appliances like washing machines, smart thermostats, and even 'enterprise computing systems' (in offices and commercial settings). Like New York's bill, Minnesota's includes a carve-out for intellectual property, clarifying that no trade secrets need to be shared by manufacturers. In sum, Minnesota's bill fills some of the loopholes that were watered down with New York's law and firmly establishes that software support and software-based tools is now a legal expectation in that state.

3.2.3. Other State R2R Laws Requiring Software Access

Beyond New York and Minnesota's general electronics statutes, several other U.S. states have pursued more specialised R2R laws that explicitly mandate access to software or firmware as part of necessary repair resources:

Colorado has been an early mover on niche R2R issues with the nation's first R2R law for medical mobility devices in 2022, the *Consumer Right to Repair Powered Wheelchairs Act*.[61] Effective 1 January 2023, the law requires a wheelchair manufacturer to provide owners and independent technicians with parts, tools, documentation, and "embedded software" needed to repair a powered (electric) wheelchair. The Act defines "embedded software" as:

> "(a) means programmable instructions provided on firmware delivered with an electronic component of equipment or with any part for the purpose of restoring or improving operation of the equipment or part; and
>
> (b) includes all relevant patches and fixes that the manufacturer makes to equipment or two any part for the purpose of restoring or improving the equipment or part."

The Act also defines tools as including "any software program…that provides, programs, or pairs a new part… or calibrates functionality." Similar to the New York and Minnesota laws, the Colorado's Act also stipulates that manufacturers do not have to divulge trade secrets as part of their obligations to provide these resources.

Building on this success, Colorado also enacted the *Consumer Right to Repair Agricultural Equipment Act* in 2023, the country's first R2R law covering farm machinery specifically.[62] Starting 1 January 2024, agricultural equipment manufacturers in Colorado must supply to farmers and independent mechanics the resources needed to repair their equipment. Those resources are defined to include "any documentation, parts, embedded software, firmware, tools… or data". The bill is unique in its approach to include "data" in the list of items that must be provided by manufacturers, including any machine-generated performance or diagnostic data needed for repairs. In essence, Colorado's agricultural R2R bill ensures that farmers have access to the same diagnostic software and firmware tools that dealers have, directly addressing software barriers and firmware restrictions that have plagued tractor and combine repairs in recent years.

Several other U.S. state laws have targeted specific product areas with R2R provisions that involve software access. This includes Massachusetts' longstanding automotive bills and the disclosure of 'vehicle data'[63], and California's *Right to Repair Act* (Senate Bill 244)[64] that addresses consumer electronics, which provide less explicit references to things like firmware, calibration programs, or other software-based tools. The overall trend reflects a growing consensus among state-level lawmakers that modern products

and devices absolutely require access to firmware, software diagnostics, and digital keys and that these resources form an essential part of R2R legal frameworks.

Together, both the United States and EU approaches to the R2R demonstrate a converging understanding (despite somewhat distinct orientations). They both make clear that access to embedded software and software-based tools is essential to enable independent repair. In both cases, manufacturers are being told that providing physical parts or components and written instructions is not sufficient. Concrete obligations to transfer or provide access to these software tools are increasingly a core component of R2R legal frameworks on both sides of the Atlantic.

4. Source Code Protections in Trade Agreements

4.1 Background & Context

Recent bilateral and plurilateral FTAs have included "e-Commerce" or "Digital Trade" chapters that restrict governments from requiring transfer or access to "source code" as a condition for market access.[65] Given the essential role of software and software-based tools, this creates a potential overarching transnational legal barrier to the successful implementation of R2R mandates at the domestic level in both the U.S. and EU. This is because FTAs are binding international treaties, and as a result, states are obligated under international law to ensure their domestic measures conform to those commitments. Therefore, where domestic laws (such as R2R statutes) conflict with FTA obligations, they create a risk of non-compliance with international commitments that could lead to disputes under the agreement and, ultimately, result in trade sanctions. Because of this, the risk of inconsistency with FTA commitments often results in national governments or legislators amending or interpreting domestic laws to avoid breaching their obligations under FTAs, or to bring measures into conformity once they have been challenged through dispute settlement.

The precise wording and implications of special source code protections vary between FTA texts, but the first clear template for these rules is found in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). The CPTPP is a large plurilateral FTA in which neither the U.S. nor the EU are parties, but which nevertheless establishes a model that has been followed by both entities in subsequent agreements. Article 14.17 of the CPTPP stipulates that:

> "No party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory"

The ban on mandated transfer or access means that governments arguably cannot impose requirements on manufacturers of devices with embedded software to transfer

or provide access to that software. This presents a significant obstacle for the proper operation of R2R laws. And though FTA source code protections occasionally include narrow exceptions (for example, to allow manufacturers to *modify* source code to comply with domestic legislation, or disclosure in the context of a judicial proceeding), the default rule is non-disclosure.[66]

4.2 Distinctions Between Source Code and Object Code

To understand the potential scope and implications of FTA source code protections it is worth briefly outlining the technical and terminological distinctions between "software", "source code", and related concepts. At a very basic level, "source code" is a representation of a computer program in human readable language.[67] It is normally the version of software as originally written by its author. For example, if a user right clicks on a webpage and selects "view page source", what is displayed serves as an instructive example of source code and its role in programming.

This can be distinguished from *object code,* which is produced when source code is translated (or "compiled") into machine-readable language understandable by a computer (i.e., ones and zeroes).[68] Source code is generally written at a high level of abstraction and therefore agnostic to the end-computing platform or hardware that it will be executed on. In contrast, object code must be tailored to a particular computer, system, virtual environment, or platform on which it is executed.

Viewed in this way, source code is analogous to the architectural blueprints of a building, detailing its design, materials, and functionality. Object code, on the other hand, reflects the building's physical components assembled into a tangible whole. It is for this reason that access to source code confers a whole host of capabilities on those who have access to it, including secondary activities and discoveries such as bug detection, error correction, modification, and enhancements.

4.3 Analysis of Key Agreements and Provisions

FTA source code protections have found their way into numerous agreements since their first intimation on the CPTPP. Some agreements have expanded on the potential scope of subject-matter that may be covered by these prohibitions, while others have included clarifying language that may help narrow their application in certain cases, including R2R policies.

4.3.1. United States-Mexico-Canada Agreement (USMCA)

Serving as an example of the more expansive approach is the *United States-Mexico-Canada* (USMCA) agreement, which at Article 19.16 provides that:

> "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."

In invoking this language, the USMCA expands upon the CPTPP approach by including "algorithm" in the subject-matter shielded from transfer or access. The USMCA's Article 19.1 defines "algorithm" as:

> "…a defined sequence of steps, taken to solve a problem or obtain a result."

This broad definition has some important implications for R2R policy. On the one hand, requiring access to a compiled binary (object code) in the form of repair software or an access key to address parts-pairing is not the same as providing *source code*. On this basis, one line of argumentation may be that software and software-based tools necessary for repair are not captured by the FTA prohibition against disclosure or access. But on the other hand, the expansion of the prohibition to '*algorithms expressed* in source code' leaves open the possibility for arguments from manufacturers that the use of access keys or repair software reveals aspects of the underlying algorithms or 'software logic', broadly construed. This line of argumentation could be used to support a more restrictive interpretation of the FTA language by manufacturers, industry groups, or government lawyers litigating trade cases that, in effect, limits access to software and software-based tools needed for repair even when they are distributed in object code.

Importantly, the USMCA also includes an important exception for investigations and inspections. Subsection (2) of Article 19.16 provides that:

> "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**…"

An important qualifier in this exception is the word "specific", which requires that a regulatory or judicial investigation be ad-hoc or outside of a general regulatory scheme to escape the FTA's general prohibition on disclosure or access. This has potentially important implications for R2R legislation such as those under the EU's ERST that envision "compliance checks" and market surveillance measures. Thus, while a general exception permitting regulatory requirements to disclose or provide access to source code would be presumably beneficial for R2R frameworks, the limitation to 'specific' proceedings is likely to significantly narrow this potential.

The potential problems for the R2R created by USMCA's approach transcends the narrow scope its exceptions, however. The potential for conflict arises not only when R2R frameworks are enforced, but also when they are enacted. Therefore, the legal requirement on manufacturers to provide software, access keys, or repair tools to third

parties could itself be seen as "requiring access to a person of another Party's algorithms" regardless of whether enforcement or investigation of those obligations is carried out by a regulatory body.

4.3.2 EU-Japan Economic Partnership Agreement (EU-Japan EPA)[69]

The EU has also included source code provisions in its more recent trade deals, though with distinctly European nuances. The EU-Japan Economic Partnership Agreement (EU-Japan EPA) was one of the first EU FTAs to include such a rule. Notably, Article 8.73 similarly prohibits state parties from requiring transfer or access to source code while also including some important caveats. The EU-Japan EPA also does not confine its prohibition on source code access or transfer to processes necessary for import, distribution, or to otherwise gain market access. The absence of this contextual qualification in the EU-Japan EPA broadens the scope and application of source code protection. On this basis, it may give product manufacturers greater justification for arguing that domestic R2R mandates requiring software disclosure inherently conflict with the terms of the agreement.

In contrast to the USMCA, the EU-Japan EPA includes a more robust set of exceptions that would permit disclosure or access to source code, including those for "commercially negotiated contracts" and for the purposes of "public procurement". But on the other hand, the EU-Japan EPA includes clarifying language that may also broaden the practical scope of what is included as "source code":

> "For greater certainty, 'source code of software owned by a person of the other Party' **includes source code of software contained in a product**."

While there is no available evidence of manufacturers relying upon this clarification to thwart the operation of R2R laws, the expansion to source code 'contained in a product' leaves open the possibility for argument by manufacturers that obliged sharing of firmware or diagnostic tools with third parties is the same as *sharing the code in that product*. As is the case with the USMCA's expansive notion of 'algorithm', the risk with the EU-Japan Agreement's embrace of source code *in products* lies in the consequences of its interpretation. And given that finished products are ordinarily sold and shipped with only object code (binaries), this could result in manufacturers arguing, in effect, that these rules extend to software tools in object code form as well. This could have important implications for devices such as the GE Smart HQ service calibration tool and the Taylor C602 soft-serve ice cream machine discussed in Part 2.

4.3.3 EU-Singapore Digital Trade Agreement (EU-Singapore DTA)[70]

In May of 2025, the EU and Singapore signed a standalone Digital Trade Agreement ("EU-Singapore DTA"), the first such digital-only agreement for the EU. This agreement follows the template of EU's recent FTAs but is focused exclusively on digital trade issues. It contains the familiar source code provision, but with some important exceptions.

Crucially, it includes a similar exception to the USMCA's regulatory or judicial investigation, but with much more permissive language:

> "[This Article] does not affect the right of regulatory, law enforcement or judicial bodies of a Party to require the modification of source code of software to comply with its laws or regulations that are not inconsistent with this Agreement"[71]

The DTA goes on to provide further carveouts and clarifications for "regulatory assessment bodies" at Article 11(3)(a):

> "[Nothing in this Article shall affect] … the right of regulatory authorities, law enforcement, judicial or conformity assessment bodies of a Party to require **transfer of, or access to**, source code of software, either prior to or following import, export, distribution…**to secure compliance with its laws or regulations pursuing legitimate public policy objectives**…"

Importantly, the carveouts for regulatory assessment bodies allow both "transfer" and "access" to source code, presumably permitting regulators to share or distribute it to third parties. In a clarifying footnote, the Agreement defines "conformity assessment body" as referring to "a relevant government body or authority of a Party…carrying out the procedures of assessment of conformity with applicable laws or regulations of that Party."

Upon a cursory reading, the EU-Singapore DTA appears to be far more permissive than the USMCA in allowing for regulators to require disclosure or access to source code beyond specific investigations or judicial proceedings. It also cedes some ground to "laws or regulations pursuing legitimate public policy objectives" and permits source code access and transfer to "secure compliance with its laws or regulations". The flexibility offered to domestic priorities and objectives seems to point in the general direction of R2R frameworks.

Pouring some cold water on this optimism, however, the conflict persists because of how domestic R2R frameworks are operationalised in practice. In general, R2R frameworks operate as broad, horizontal consumer rights regimes. They apply to all consumers and businesses rather than to discrete enforcement or compliance functions of governments or state bodies. As such, even though the EU-Singapore DTA exceptions evoke greater flexibility, the continuous and universal character of R2R frameworks would likely fall outside of the narrow, ad-hoc enforcement context contemplated by this more permissive exception framework. In practice, therefore, this means that despite its more flexible wording, the exception is unlikely to shield comprehensive R2R legislation from conflict with the underlying FTA prohibition on source-code disclosure.

4.3.4 Development of Policy Positions

The above demonstrates a clear trend toward incorporating source code protection clauses into FTAs among advanced economies.[72] Furthermore, parallel to these bilateral and regional FTAs, dozens of countries have also attempted to craft multilateral digital trade rules through the World Trade Organization. In 2019, a large coalition of WTO members launched the Joint Statement Initiative (JSI) on Electronic Commerce, aiming to negotiate global disciplines on e-commerce and digital trade.[73] By 2023, JSI talks had attracted over 90 economies (including major players like the EU, US, Japan, and China).

The larger policy shift and turning point in these trends came in late 2023 when the United States made a surprise policy reversal that fundamentally shifted the JSI dynamics. USTR Katherine Tai withdrew several U.S. proposals that had been on the table since 2019, including the rules requiring unrestricted data glows and prohibiting mandated access to source code.[74] Essentially, Washington dropped its longstanding demands for binding WTO commitments on free data movement and source code protections. The USTR's statement on this point was brief, stating that:

> "Many countries, including the United States, are examining their approaches to data and source code, and the impact of trade rules in these areas. In order to provide enough policy space for those debates to unfold, the United States has removed its support for proposals that might prejudice or hinder those domestic policy considerations…"

Core to these 'domestic policy considerations' have been addressing anti-competitive activity in the digital economy, including issues like the R2R.[75] In a letter thanking President Biden for the USTR's reversal on digital trade, a group of senators and house representatives noted that source code and algorithm secrecy risked gutting "right-to-repair laws being enacted in states nationwide", urging keeping policy space for domestic tech regulation.[76] At present, the U.S. position on digital trade (and FTA source code protections in particular) remains in the process of recalibration, and this pivot from its initial leadership role acknowledges the need to reevaluate the potential impact of these rules. Indeed, if domestic R2R frameworks are to fulfil their normative and operational goals, overarching trade commitments cannot pre-empt clear obligations on manufacturers to provide reasonable access to software and software-based tools.

The EU, for its part, has been actively advancing its own digital trade agenda; albeit with a somewhat distinct philosophy from the United States. Though the EU had historically been more hesitant than the U.S. to embrace sweeping e-commerce provisions (given its commitment to privacy and confidentiality)[77], it has since more fully championed digital trade chapters. The EU is motivated (in part) by the need to ensure a secure strong consumer protections for consumers in the digital environment, reflecting

its inclination toward broad-based regulation of technology firms. This is codified in the European Commission's 2021 trade strategy, which makes supporting Europe's "digital agenda" a priority for trade policy.[78] As a result, contemporary EU trade agreements such as the EU-Singapore agreement commonly contain self-standing chapters on digital trade, with source code protections permitting regulatory oversight included.

In looking at the larger and international picture that results from these trends, the outcome on source code provisions remains uncertain, but there is room for optimism.[79] As a positive development, the JSI's final slimmed-down agreement now excludes the controversial source code clause.[80] At the same time, the fact that a sizable group of WTO members were willing to negotiate such rules prior to the U.S. reversal evidence broader international interest in source code protections, at least to some extent. It is therefore conceivable that outside the WTO, smaller plurilateral agreements will carry forward some iteration of these rules (for example, as part of expansion of the CPTPP membership). Furthermore, there remains the possibility for new alliances of the willing, with groups of countries that may agree on broader digital economy pacts under the OECD framework or as standalone treaties.

On the other hand, much has changed since the first iteration of FTA source code protections were introduced as part of the CPTPP and reformulated as part of the USMCA. The burgeoning growth of the R2R movement and economic circularity have given policymakers reason to stop and rethink many of their economic and industrial policies since the COVID-19 pandemic. Furthermore, the growing interest and concern in algorithmic governance and the societal impacts of persuasive technologies and platforms lean heavily toward greater scepticism of these rules as we move into the future. Taking an even larger view, shifting geopolitical dynamics are increasingly requiring countries to pursue protectionist strategies relating to their markets and national security. Each of these factors suggest that national lawmakers and trade negotiators will assess FTA source code protections with greater scrutiny in the months and years ahead.

5. Outstanding Issues & Ambiguities

When analysing the source code protection language in recent FTAs in light of domestic R2R frameworks in the United States and the EU, there are a number of uncertainties and ambiguities that become apparent:

Do R2R frameworks require transfer or access to "source code"?

R2R frameworks on both sides of the Atlantic are generally agnostic to whether software or software-based tools must be distributed in object code or source code form. In many cases, such as New York's *Digital Fair Repair Act,* legislation expressly excludes any obligation that would result in the disclosure of trade secrets. This suggests that manufacturers are not expected to share source code. Nevertheless, when where FTAs

refer only to “source code of software” without mentioning “algorithms” or “software contained in products”, a baseline interpretive risk remains. The act of requiring manufacturers to provide diagnostic software, firmware updates, or calibration programs could be construed as requiring “access to source code” insofar as these software-based tools are intimately connected to, and often derived from, the manufacturer’s proprietary code.

That risk is materially amplified where FTA language extends beyond source code itself to cover “algorithms” or “software contained in products”, such as in the USMCA and the EU-Japan agreements. These formulations expand the protected subject matter from human-readable code to the functional logic of software and its embedded implementations. This increases the likelihood that repair software or access keys (typically distributed in object form) could be characterised as falling within the scope of the prohibition. In such cases, the FTA’s non-disclosure rule could more readily be invoked to pre-empt domestic R2R laws that require manufacturers to provide software-based repair tools, even when no access to source code *per se* is sought.

Pre-emption of domestic law

As addressed in Part 4 above, trade agreements are binding on states and their governments, but they do not automatically invalidate domestic laws in the way a national constitutional court might. Instead, enforcement occurs through state-to-state dispute mechanisms. This means that a government can be held internationally responsible for breaching its treaty obligations, but the domestic R2R statute remains formally in force unless the state chooses to amend or repeal it. For this reason, FTAs with restrictive source code protections are unlikely to directly strike down domestic R2R legislation.

However, a state found in violation could face international dispute-settlement proceedings, either under an FTA’s own mechanism or at the WTO. This could lead to retaliation, compensation claims, or negotiated settlements. In practice, the prospect of such proceedings (or persistent complaints from trade partners) can exert strong diplomatic and economic pressure on governments to narrow or revise their R2R rules to ensure conformity. This indirect but potent form of pre-emption may, over time, lead to the softening or erosion of R2R frameworks at the U.S. state level or to narrower interpretations of EU Directives and Regulations to avoid potential trade conflicts.

Beyond pressures applied once R2R frameworks come into force, pre-enactment trade law compliance also could play a significant role in shaping future laws. Within the EU, legislative and regulatory bodies often vet new policy proposals to ensure their compatibility with existing trade commitments. This can lead to the dilution or narrowing of initial R2R ambitions. For example, during the drafting of the EU *Artificial Intelligence Act,* the EU Commission’s Directorate-General for Trade reportedly urged the Directorate-General for Justice to limit provisions allowing regulators to access source code because

of the EU's commitments under the EU-UK Trade and Cooperation Agreement.[81] This type of international coordination illustrates that trade law obligations can constrain domestic policy design *ex ante*, even before any international dispute arises.

Exceptions for regulatory bodies, proceedings, and investigations

Many of the FTAs surveyed above include exceptions that allow some form of transfer or access to source code for particular public-interest purposes, regulatory processes, and other procedures. These exceptions vary significantly in their scope and potential application to R2R frameworks. Where R2R legislation imposes general obligations on manufacturers to provide access to software and software-based tools, it is not clear that these measures would be captured by the general exceptions for "regulatory assessment bodies". This is because statutory obligations on manufacturers that are enforced through private litigation are not "regulatory" in a strict sense. On the other hand, where R2R frameworks include oversight by administrative authorities to ensure compliance and enforcement with these standards, they are more likely to be saved by the exemptions found in various FTAs.

In practice, however, these exceptions are difficult for domestic regulators to operationalise. Triggering them would normally require an authority to issue a formal request for information or access to source code in connection with a specific investigation or compliance verification. Yet, most domestic regulators responsible for R2R frameworks and consumer protection are neither mandated nor resources to invoke trade-law exceptions in the first place. They may also be unaware of this possibility entirely. Therefore, even where FTAs may be interpreted to technically permit source code access or disclosure for specific regulatory purposes related to the R2R, these clauses are unlikely to be an effective solution for broad-based, horizontal R2R consumer frameworks.

6. Weighing the Potential Paths Forward

Amendments to Domestic R2R Frameworks

One approach to resolving potential conflicts and ambiguities may be to amend domestic R2R frameworks to include clarifying provisions. This could, for instance, involve interpretive clarifications that obligations on manufacturers to provide software or software-based tools does not imply the obligation to divulge "source code" or "algorithms" in contravention of any trade agreement. This would fall short of a satisfactory resolution, however, for at least three reasons. The first is that this would come at the cost of potentially weakening the scope of R2R legislation's application to certain software-based tools that the manufacturer asserts constitute 'source code'. In other words, this would leave manufacturers largely in charge of deciding which tools are subject to R2R regulation and which are not. Secondly, this approach would fail to resolve the definitional and conceptual ambiguities that are present across various FTAs,

including the application of exemptions for public interest regulatory processes and related investigations. Finally, the process of amending numerous domestic R2R laws substantially increases the likelihood of dis-harmonisation while providing the opportunity for industry lobbying to weaken the effectiveness of these laws over the long term.

Relying on Existing Public Interest Exemptions in FTAs

Domestic lawmakers and R2R advocates may alternatively set their sights on the existing exemptions in FTAs for public interest regulatory oversight and formulate arguments that R2R frameworks fall within their scope. While some agreements contain exemptions that could apply to certain approaches to R2R policy, there is significant deviation. For example, the EU-New Zealand agreement permits only "access" to source code as part of regulatory exemptions, whereas the EU-Singapore DTA permits both "transfer" and "access". This distinction is essential, because the proper operation of R2R policy involves manufacturers sharing and distributing software and software-based tools to consumers and independent repairers (third parties). This necessarily requires more than regulatory bodies 'accessing' source code, but also widespread disclosure and provision for the benefit of others. This lack of uniformity results in the existing exemptions in FTA frameworks being inadequate for R2R policy. They are neither consistent enough to cover the various approaches to R2R policy nor broad enough to address the need to share software and software-tools with the public and third-party repairers.

Recalibrating Trade Policy to Support the R2R

Likely the most productive and effective approach to resolving these tensions is to advocate for a recalibration of digital trade policy to abandon source code protections entirely. Even beyond the R2R, the potential societal and democratic risks of preventing access and transfer to source code is simply too high. Where algorithmic and software-enabled products and services are having an increased impact on social and democratic processes, trade negotiators should not be tying the hands of national lawmakers to craft policy that safeguards the public interest and national security. Similar to the R2R, this will inevitably require access to source code.

If FTA source code protections are to remain, specific carveouts are needed for R2R frameworks given that they operate as much more than mere compliance and enforcement schemes. Providing room for optimism in this latter strategy is the EU's willingness to include increasingly permissive exemptions in recent FTAs[82] along with the United States' reversal and re-evaluation of its broader approach to digital trade. The structure and approach to these exceptions must be significantly broadened, however, if the R2R is to be embraced by them in future deals.

At present, the United States is in the process of renegotiating the USMCA and reevaluating a large number of its trade relationships around the world. This presents an

opportunity to craft a new approach to digital trade that either removes prohibitions on source code disclosure entirely or includes a clause carving out the sharing of software and software-based tools for legitimate repair, safety, or environmental purposes. Though no FTA at present currently includes a R2R-specific carveout in relation to digital trade and source code, future texts could be crafted with exceptions for the "maintenance of products" and the "safety of consumers" that shelter R2R laws and allow mandated access *and* transfer to software and source code beyond isolated investigations or as part of broader regulatory schemes.

7. Conclusion

The global proliferation of FTA source code protections has created a new and underappreciated layer of complexity for the R2R. Domestic laws in the EU and the United States now mandate access to software and software-based tools that are essential for repair. At the same time, digital trade agreements often define protected source code in such a way that can be interpreted to insulate these tools from disclosure to third parties. These competing regulatory currents appear to be on a collision course.

The report shows that although R2R laws do not generally demand source code explicitly, their obligations to provide firmware, calibration software, diagnostic applications, and digital keys can be position by manufacturers as encroaching on trade secrecy protection that is now enshrined in many FTAs. Ambiguous drafting (such as the inclusion of "algorithms" in the USMCA or clarifications about source code "contained in products" in the EU-Japan EPA) heightens the risk of overbroad interpretation. At the same time, international trade policy is undergoing a period of immense change. The United States has paused its promotion of rigid digital trade rules, opening space to consider new models, values, and priorities. The EU continues to export its digital trade agenda, but its agreements have increasingly incorporated exceptions that permit regulatory oversight and public interest measures. This convergence signals an opportunity for recalibration of digital trade and source code protections writ large.

Going forward, policymakers and trade representatives on both sides of the Atlantic should work to find links and points of common interest between digital trade rules and R2R mandates. The most direct and effective approach would be to remove FTA source code protection clauses altogether. Alternatively, explicit carve-outs for repair, maintenance, and consumer safety could reconcile these competing objectives as part of a broader ratcheting down of trade protections that impact software-related innovation. Without such adjustments, well-resourced manufacturers and lobbying efforts may leverage trade law to resist or dilute R2R obligations, thereby weakening the enormous hard-fought gains to environmental sustainability, consumer protection, and market competition.

In sum, the path forward requires better aligning trade and R2R policy. By modernising trade provisions to recognise repair as a legitimate public interest objective, and in recognising the crucial role of software and software-based tools, governments can safeguard both technological innovation and the ability for consumers and independent repairers to fix and maintain the products they own.

---

* Assistant Professor of Law & Computer Science, Dalhousie University (Canada); Doctoral Researcher in Law, European University Institute (Italy), anthony.rosborough@dal.ca

[1] As is explained in greater detail in Part 4, some agreements do not explicitly confine special protections against source code access or transfer to reviews or government processes that are conditional for market access. Older EU agreements tend to phrase the obligation more generally: "A Party may not require the transfer of, or access to, source code of software…" This could be interpreted much more broadly and could mean that any law or regulation that seeks to obtain access or transfer of source code can be challenged as inconsistent with the FTA. See, *Agreement between the European Union and Japan for an Economic Partnership* (OJ L 330, 27 December 2018) art 8.73.

[2] "Firmware" is a subset of software that is often embedded in hardware devices and provides low-level controls and direct hardware functionality. Users familiar with earlier iterations of Windows may recall updating "drivers" for various hardware peripherals like printers or scanners. Firmware plays a similar role in modern smart technologies and products. The distinction between software and firmware is therefore less technical than it is situational. Firmware refers to software that is devoted to performing a particular role, interacting closely with hardware to manage fundamental operations.

[4] Directive (EU) 2024/1799 of the European Parliament and of the Council of 13 June 2024 on common rules promoting the repair of goods and amending Regulation (EU) 2017/2394 and Directives (EU) 2019/771 and (EU) 2020/1828, OJ L, 2024/1799, 10.7.2024

[5] Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for setting ecodesign requirements for sustainable products (the "ESPR") (amending Directive 2020/1828 and Regulation 2023/1542, and repealing Directive 2009/125/EC), OJ L, 2024/1781, 28.6.2024.

[6] Commission Regulation (EU) 2023/1670 of 16 June 2023 laying down ecodesign requirements for smartphones, mobile phones other than smartphones, cordless phones and slate tablets, OJ L 214, 31.8.2023, p. 47.

[7] *Digital Fair Repair Act*, N.Y. Gen. Bus. Law § 399-nn (enacted via Senate Bill S4104A / Assembly Bill A7006B) (signed December 28, 2022, effective December 28, 2023).

[8] *Digital Fair Repair Act*, Minn. Stat. § 325E.72 (2023) (effective July 1, 2024).

[9] *Consumer Right to Repair Digital Electronic Equipment*, Colorado HB 24-1121 (signed by Governor, expanding RT Repair statutes to include digital electronics).

[10] For example, as early as the 1920s, industrial pioneer Henry Ford emphasised repairability as a design goal for Ford vehicles. See, Masayuki Hatta, 'The Right to Repair, the Right to Tinker, and the Right to Innovate' (2020) 19 Annals of Business Administrative Science 143–157 https://doi.org/10.7880/abas.0200604a accessed 6 July 2025.

[11] One of the earliest legislative developments enshrining the Right to Repair in the United States was Massachusetts automotive right to repair bill, *An Act protecting motor vehicle owners and small businesses in repairing motor vehicles*, H.4362 (Mass, 187th Gen Ct, enacted 8 July 2012) (signed 8 July 2012).

[12] Emma Bowman, "A new copyright rule lets McDonald's fix its own broken ice cream machines" (3 November 2024) NPR, online: https://www.npr.org/2024/11/02/g-s1-31893/mcdonalds-broken-ice-cream-machine-copyright-law, accessed 30 August 2025.

[13] Ashley Belanger, "Trains were designed to break down after third-party repairs, hackers find" (13 December 2023) Ars Technica, online: https://arstechnica.com/tech-policy/2023/12/manufacturer-deliberately-bricked-trains-repaired-by-competitors-hackers-find/ accessed 30 August 2025.

[14] See, Anthony D Rosborough, "A Conceptual Map of the Right to Repair: Where Upcycling Fits In" in Peter Mezei & Heidi Härkönen, *Research Handbook of Intellectual Property and Upcycling* (Cambridge University Press, 2026) [Forthcoming].

[15] European Parliament, 'New EU rules encouraging consumers to repair devices over replacing them' (Press Release, 21 November 2023) https://www.europarl.europa.eu/news/en/press-room/20231117IPR12211/new-eu-rules-encouraging-consumers-to-repair-devices-over-replacing-them accessed 28 August 2025.
[16] See, for example, Minnesota's 2023 Digital Fair Repair Act (now Minn. Stat. § 325E.72), which requires OEMs to provide "documentation, parts, and tools, inclusive of any updates to … embedded software" to owners and independent repairers, and (where a device has an electronic security lock) to provide the special documentation, tools, and parts needed to reset the lock, which may be supplied via a secure release system.
[17] Kyle Wiggers, "New York's right-to-repair bill has major carve-outs for manufacturers" (3 January 2023) Tech Crunch, online: https://techcrunch.com/2023/01/03/new-yorks-right-to-repair-bill-has-major-carve-outs-for-manufacturers/ accessed 3 September 2025.
[18] Sam Metz, "Big tech and independent shops clash over 'right to repair' (30 March 2021) *AP News,* online: https://apnews.com/article/legislature-nevada-coronavirus-pandemic-laws-5ade405a7befdf16e9f0107b7e142be3, accessed 2 Sept 2025.
[19] Examples include automakers' lawsuit against Massachusetts' vehicle data access law (*Alliance for Automotive Innovation v Cambell*) where the trade group sought to block the state's law expanding independent wireless access to telematics mechanical data on the grounds that is pre-empted national traffic and motor vehicle safety legislation. See, Dallin R Wilson, "Judge Denies Industry Challenge to Massachusetts Data Access Law" (11 February 2025) Sayfarth https://www.seyfarth.com/news-insights/judge-denies-industry-challenge-to-massachusetts-data-access-law.html, accessed 28 July 2025. Agricultural equipment manufacturer John Deere's Memorandum of Understanding with the National Farm Bureau is an example of where a voluntary agreement on the manufacturers' terms was sought to avoid prescriptive regulation that would have obliged the company to provide access to its proprietary software tools to farmers.
[20] Michael Fridelwald & Oliver Raabe, "Ubiquitous computing: An overview of technology impacts" (2011) 28:2 Telematics and Informatics 55-65, 55.
[21] Bruno Dorsemaine, Jean-Philippe Gaulier, Jean-Philippe Wary, Nizar Kheir and Pascal Urien, 'Internet of Things: A Definition and Taxonomy' (9-11 September 2015) in *Proceedings of the 9th International Conference on Next Generation Mobile Applications, Services and Technologies* 72–77 (IEEE) doi:10.1109/NGMAST.2015.71
[22] IoT Business News, 'State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally' (IoT Business News, 4 September 2024) https://iotbusinessnews.com/2024/09/04/26399-state-of-iot-2024-number-of-connected-iot-devices-growing-13-to-18-8-billion-globally/ accessed 6 July 2025.
[23] See, Kyle Wiens, "You Gotta Fight For Your Right to Repair Your Car" (13 February 2014) The Atlantic, online: https://www.theatlantic.com/technology/archive/2014/02/you-gotta-fight-for-your-right-to-repair-your-car/283791/ where the iFixit co-founder writes "You can't fix a computer with a wrench. Instead, fixing modern cars requires special diagnostic tools and official service information – information that some manufacturers don't share with independent repair techs…"
[24] Maddie Stone, "Apple uses software to control how phones get fixed. Lawmakers are pushing back." (30 January 2024) Grist, online: https://grist.org/technology/apple-uses-software-to-control-where-phones-get-fixed-lawmakers-are-pushing-back/ accessed 1 July 2025.
[25] Gay Gordon-Byrne, 'Apple's War on Right to Repair Through Serial Numbers' (The Repair Association Blog, 25 September 2023) https://www.repair.org/blog/2023/9/25/apples-war-on-right-to-repair-through-serial-numbers accessed 13 September 2025.
[26] Apple, "Apple to expand repair options with support for used genuine parts" (11 April 2024), online: https://www.apple.com/newsroom/2024/04/apple-to-expand-repair-options-with-support-for-used-genuine-parts/, accessed 5 July 2025.
[27] Lauren Grenlee, "How Parts Pairing Kills Independent Repair" (17 January 2023) iFixit, online: https://www.ifixit.com/News/69320/how-parts-pairing-kills-independent-repair, accessed 1 July 2025.

[28] Platform Security Summit, 'Guarding Against Physical Attacks: The Xbox One Story — Tony Chen, Microsoft' (YouTube, 21 October 2019) https://www.youtube.com/watch?v=U7VwtOrwceo accessed 12 September 2025.
[29] Jean-Philippe Pomerleau, "VIN Lock: A Barrier to the Evolution of the Automotive Industry?" (15 January 2025) L'Automobile, online: https://www.lautomobile.ca/en/mechanics/vin-lock-a-barrier-to-the-evolution-of-the-automotive-industry accessed 2 September 2025.
[30] "VIN locking" is related to the concept of "VIN burning", which is the practice of limiting a vehicle electronic control unit (ECU) or central computer to function with a single vehicle identification number or VIN. This allows the manufacturer to constrain the utility of a replacement part to work with only one particular vehicle. For a more fulsome explanation of these techniques, see Federal Trade Commission, *Nixing the Fix: An FTC Report to Congress on Repair Restrictions* (May 2021), 23 https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf accessed 13 September 2025
[31] For an up-to-date registry of operational and broken McDonald's ice cream machines, visit McBroken https://mcbroken.com/ accessed 13 September 2025.
[32] Andy Greenberg, "They Hacked McDonald's Ice Cream Machines – and Started a Cold War" (20 April 2021) Wired, online: https://www.wired.com/story/they-hacked-mcdonalds-ice-cream-makers-started-cold-war, accessed 20 August 2025.
[33] Taylor Company, *Model C602 Combination Shake/Soft Serve Freezer: Service Manual* (Original Service Instructions 057888-S, January 2007; updated 14 July 2023) https://dslinc.com/wp-content/uploads/2024/12/C602.pdf accessed 13 September 2025.
[34] Andy Greenberg, "The McDonald's ice Cream Machine Hacking Saga Has a New Twist" (23 November 2021) Wired, online: https://www.wired.com/story/mcdonalds-ice-cream-machine-hacking-kytch-taylor-internal-emails/ accessed 10 July 2025.
[35] Linda Xu & Ian Drew, "The great McDonald's ice cream machine meltdown: copyright, control, and the fight for repair rights" (28 February 2025) Davis Collision Cave, online: https://dcc.com/news-and-insights/the-great-mcdonalds-ice-cream-machine-meltdown-copyright-control-and-the-fight-for-repair-rights/ accessed 8 July 2025.
[36] For example, since the 1990s, virtually all cars produced globally have standardised on-board diagnostic ports ("OBD-II") that allow reading basic diagnostic trouble codes with generic scanners.
[37] For example, Volkswagen's "ODIS" (Offboard Diagnostic Information System) is the official, dealer-level diagnostic software used by the Volkswagen Group to diagnose, repair, and program all its vehicle brands including VW, Audi, Skoda, and SEAT. This system connects directly to the manufacturer's German servers to provide technician with up-to-date fault codes, technical service bulletins, wiring diagrams, and other information. See, Technical Topics, 'ODIS VW Group Diagnostic Tool' (Technical Topics) https://techtopics.co.uk/odis-vw-group-diagnostic-tool/ accessed 13 September 2025.
[38] Maria Merano, "Tesla diagnostic software now available for purchase in the US" (26 August 2021) Teslarati, online: https://www.teslarati.com/tesla-diagnostic-software-right-to-repair-service/#:~:text=,greentheonly%29%20August%2026%2C%202021 accessed 10 September 2025.
[39] Jason Koebler, 'This Is Apple's Mysterious "iPhone Calibration Machine"' (VICE, 14 March 2017) https://www.vice.com/en/article/this-is-apples-mysterious-iphone-calibration-machine/ accessed 13 September 2025.
[40] Kevin Purdy, 'Here Are the Secret Repair Tools Apple Won't Let You Have' (iFixit, 28 October 2019) https://www.ifixit.com/News/33593/heres-the-secret-repair-tool-apple-wont-let-you-have accessed 13 September 2025.
[41] Apple Support, 'Use Repair Assistant to finish an iPhone or iPad repair' (2 April 2025) https://support.apple.com/en-us/120579 accessed 13 September 2025
[42] One example of a lesser-known software tool of this sort is Samsung's "Must" application that is required for calibration and diagnostics on the manufacturer's Galaxy line of phones. For more on this, see Pr0Ankit, 'How to calibrate Force Touch on Samsung Galaxy S8' (XDA Developers Forum, 18 January 2018) https://xdaforums.com/t/how-to-calibrate-force-touch-on-samsung-galaxy-s8.3736990/ accessed 13 September 2025.
[43] SmartHQ Pro, 'Appliance Diagnostic Platform | SmartHQ™ Service' (SmartHQ Pro) https://www.smarthqpro.com/service accessed 13 September 2025.

[44] SmartHQ Pro, 'Quick Start Guide: SmartHQ™ Service Setup' (SmartHQ Pro) https://www.smarthqpro.com/service/quick-start-guide accessed 13 September 2025.
[45] 'Refrigerator Diagnostics using the Updated SmartHQ Service Platform' (YouTube) https://www.youtube.com/watch?v=TjCLA0ydmoQ accessed 13 September 2025.
[46] Elizabeth Chamberlain, 'Repairing a Fridge Costs More Than a Fridge' (iFixit, 23 November 2022) https://www.ifixit.com/News/69391/repairing-a-fridge-costs-more-than-a-fridge accessed 13 September 2025.
[47] *Consolidated Version of the Treaty on the Functioning of the European Union* [2012] OJ C 326/47, art 26 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF accessed 14 September 2025.
[48] Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC [2024] OJ L, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1781 accessed 10 September 2025.
[49] Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products [2009] OJ L 285/10 https://eur-lex.europa.eu/eli/dir/2009/125/oj/eng accessed 10 September 2025.
[50] European Commission, 'Annexes 1–8 to the Proposal for a Regulation of the European Parliament and of the Council establishing a framework for setting ecodesign requirements for sustainable products and repealing Directive 2009/125/EC' COM(2022) 142 final, 30 March 2022 https://eur-lex.europa.eu/resource.html?uri=cellar:bb8539b7-b1b5-11ec-9d96-01aa75ed71a1.0001.02/DOC_2&format=PDF accessed 10 September 2025.
[51] More specifically, Annex II includes household washing machines, dryers, refrigerators, electronic displays, welding equipment, vacuum cleaners, servers and data storage products, mobile phones and tablets, and 'goods containing light means of transport batteries'.
[52] Importantly, these obligations under article 5 of the R2R Directive are limited to a relatively narrow group of products listed in Annex II. Those include household washing machines, dishwashers, refrigerators, electronic displays, welding equipment, vacuum cleaners, severs and data storage equipment, mobile phones and tables, electric bikes and scooters.
[53] Commission Regulation (EU) 2023/1670 of 16 June 2023 laying down ecodesign requirements for smartphones, mobile phones other than smartphones, cordless phones and slate tablets pursuant to Directive 2009/125/EC and amending Commission Regulation (EU) 2023/826 [2023] OJ L 214/47 https://eur-lex.europa.eu/eli/reg/2023/1670/oj/eng accessed 10 September 2025.
[54] US Congress, 'Fair Repair Act' H.R. 4006, 117th Congress (2021–2022) (introduced 17 June 2021) https://www.congress.gov/bill/117th-congress/house-bill/4006 accessed 10 September 2025.
[55] For example, in 2021 the Federal Trade Commission (FTC) issued a policy statement committing to enforce against illegal repair restrictions, following a report that found many manufacturer-imposed repair barriers (like software locks) to be anti-competitive. Furthermore, President Biden's Executive Order 14036 (2021) also encouraged the FTC to address undue repair restrictions.
[56] U.S. PIRG, 'RELEASE: All 50 states now have filed Right to Repair legislation over last 8 years' (PIRG Media Center, 24 February 2025) https://pirg.org/media-center/release-all-50-states-now-have-filed-right-to-repair-legislation-over-last-8-years/ accessed 10 September 2025.
[57] New York State Senate Bill S1320, 2023–2024 Regular Session, 'Relates to the sale of digital electronic equipment …' https://www.nysenate.gov/legislation/bills/2023/S1320 accessed 10 September 2025.
[58] Minnesota Statutes § 325E.72 (2024) ('Digital Fair Repair Act') https://www.revisor.mn.gov/statutes/cite/325E.72 accessed 10 September 2025.
[59] Ibid, subd 6 (Exclusions).
[60] Nathan Proctor, "Minnesota passes broadest Right to Repair measure to date" (24 May 2023) PIRG, https://pirg.org/articles/minnesota-passes-broadest-right-to-repair-measure-to-date, accessed 10 September 2025.
[61] Colorado House Bill HB22-1031, 2022 Regular Session, 'Consumer Right To Repair Powered Wheelchairs' https://leg.colorado.gov/sites/default/files/2022a_1031_signed.pdf accessed 10 September 2025.

[62] Colorado House Bill HB23-1011, 2023 Regular Session, 'Consumer Right To Repair Agricultural Equipment' https://leg.colorado.gov/sites/default/files/2023a_1011_signed.pdf accessed 10 September 2025.
[63] Massachusetts, Acts 2013, ch 165, *An Act relative to automotive repair* https://malegislature.gov/Laws/SessionLaws/Acts/2013/Chapter165 accessed 10 September 2025; Massachusetts, Acts 2020, ch 386, *An Act to enhance, update and protect the 2013 motor vehicle right to repair law* https://malegislature.gov/Laws/SessionLaws/Acts/2020/Chapter386 accessed 10 September 2025.
[64] California, Senate Bill 244 (2023–2024 Reg Sess), 'Right to Repair Act', ch 704, Statutes of 2023 https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB244 accessed 10 September 2025.
[65] Daniel Rangel and Katie Hettinga, 'How Federal Trade Deals Threaten States' Crackdowns on Big Tech' (Governing, 17 September 2024) https://www.governing.com/policy/how-federal-trade-deals-threaten-states-crackdowns-on-big-tech accessed 20 July 2025.
[66] Magdalena Słok-Wodkowska & Joanna Mazur, "Secrecy by Default: How Regional Trade Agreements Reshape Protection of Source Code" (2022) 25 Journal of International Economic Law 91 at 96–98.
[67] "Source Code Definition", *Linux Information Project* (14 February 2006), online: <https://www.linfo.org/source_code.html#:~:text=Source%20code%20(also%20referred%20to,human%20readable%20alphanumeric%20characters>
[68] Daniel Lin, Matthew Sag & Ronald S. Laurie, "Source Code versus Object Code: Patent Implications for the Open Source Community" (2002) 18:2 Santa Clara Computer & High Tech LJ 235–258 at 238.
[69] *Agreement between the European Union and Japan for an Economic Partnership* [2018] OJ L 330/3, art 8.73 https://eur-lex.europa.eu/eli/agree_internation/2018/1907/oj/eng accessed 8 September 2025
[70] *Agreement on Digital Trade between the European Union and the Republic of Singapore* (signed 7 May 2025) art 11 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0022 accessed 8 September 2025.
[71] Ibid article 11(2)(c).
[72] For example, a similar source code provision is found in the EU-UK Trade and Cooperation Agreement (2020). See, *Trade and Cooperation Agreement between the United Kingdom of Great Britain and Northern Ireland and the European Union* (signed 30 December 2020) art 207 https://assets.publishing.service.gov.uk/media/608ae0c0d3bf7f0136332887/TS_8.2021_UK_EU_EAEC_Trade_and_Cooperation_Agreement.pdf accessed 8 September 2025.
[73] World Trade Organization, "Joint Statement on E-Commerce", <https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm> accessed 8 September 2025.
[74] David Lawder, "US drops digital trade demands at WTO to allow room for stronger tech regulation" (25 October 2023) Reuters, online: https://www.reuters.com/world/us/us-drops-digital-trade-demands-wto-allow-room-stronger-tech-regulation-2023-10-25/ accessed 8 September 2025.
[75] For example, in presentations immediately following the U.S. reversal, Ambassador Tai commented that the USTR's concerns were influenced heavily by market competition, firm size, and other anti-trust considerations, indicating a novel confluence of policy considerations in the context of international trade. For a deeper analysis of these dynamics, see Alex Mastorides, "One Step Forward, Two Steps Back: The United States' New Direction on Digital Trade" (2025) 26:1 Minnesota Journal of Law, Science and Technology 116-203, 170-171.
[76] Elizabeth Warren, Jan Schakowsky et al., 'Letter to President Biden in Support of USTR Digital Trade Work' (6 November 2023) https://www.warren.senate.gov/imo/media/doc/FINAL%20Letter%20to%20Biden%20in%20Support%20of%20USTR%20Digital%20Trade%20Work.pdf accessed 8 September 2025.
[77] Kenneth Propp, "Transatlantic Digital Trade Protections: From TTIP to 'Policy Suicide'?" (16 February 2024) LawFare, online: https://www.lawfaremedia.org/article/transatlantic-digital-trade-protections-from-ttip-to-policy-suicide, accessed 8 September 2025.
[78] European Commission, 'Digital trade' https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/goods-and-services/digital-trade_en accessed 8 September 2025.

[79] Henry Gao, 'The Joint Statement on E-commerce: Is This Glass Half Empty or Half Full?' (Centre for International Governance Innovation, 30 September 2024) https://www.cigionline.org/articles/the-joint-statement-on-e-commerce-is-this-glass-half-empty-or-half-full/ accessed 8 September 2025.
[80] World Trade Organization, 'Joint Statement Initiative on Electronic Commerce: Communication from the Co-Convenors (Australia, Japan and Singapore)' INF/ECOM/87 (26 July 2024) https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/87.pdf&Open=True accessed 8 September 2025.
[81] Samuel Stolton, "How trade commitments narrowed EU rules to access AI's source codes," Euractiv (17 January 2024) https://www.euractiv.com/news/how-trade-commitments-narrowed-eu-rules-to-access-ais-source-codes/ accessed 7 October 2025.
[82] For example, the EU-New Zealand agreement serves as an example of an increasingly permissive and public-interest facing approach to digital trade and 'source code' provisions negotiated recently by the EU.