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.