rethink TRADE

AMERICAN ECONOMIC LIBERTIES PROJECT

Big Tech's Ploy to Internationally Preempt AI Safety and Kids' Online Safety Policy Worldwide Using Trade Agreements

And How U.S.-Mexico-Canada Agreement Renegotiations Are a Line of Defense

November 2026

DIGITAL TRADE BRIEFING PAPERS SERIES

RETHINK TRADE

rethinktrade.org

Introduction

Every day, concerns grow over the threats posed by artificial intelligence. At the same time, U.S. courts have begun to impose liability for harms from kids' exposure to social media platforms. And Congress and state legislatures are finally beginning to address emerging technology risks.

Independent auditing is emerging as a critical tool in most AI safety proposals. Illinois' Artificial Intelligence Safety Measures Act, enacted mid-2026 and widely seen as the most ambitious state-level answer yet to AI risks, requires large frontier AI developers to undergo independent third-party audits annually. The FRONTIER Act, introduced in the 119th Congress, also requires such independent evaluations. These policies recognize that real oversight of powerful AI systems requires more than companies simply attesting that their models are safe. Independent auditors need meaningful access to systems they are evaluating, including information about how models are built and operated. That may well include access to algorithms and underlying source code that create and direct the models.

However, so-called 'digital trade' rules that Big Tech interests have pushed into some recent trade agreements explicitly forbid governments from requiring access by independent auditors to key information. Countries are required to conform their domestic policies to trade-pact terms with strong internal enforcement mechanisms that can result in tariffs and other penalties on countries that do not comply. These rules can impose constraints on domestic policymaking in multiple nations in one fell swoop and chill attempts to rein in AI and social media platforms.

The 2020 U.S.-Mexico-Canada Agreement (USMCA) includes an extreme version of this international preemption ploy. It also is the only enforceable U.S. pact that has special secrecy guarantees for digital firms and products. This memo focuses on the USMCA rule that poses the greatest threat to AI safety and kids' online safety, **Article 19.16**. This broad "Source Code" obligation limits governments from requiring access to source code and other algorithmic information. It poses obvious conflicts for AI safety and social media regulation, where auditing, transparency, and oversight requirements may require companies to disclose detailed descriptions of a system's design, methodologies, or operation.

Tech lobbyists are pushing governments worldwide to adopt this USMCA rule in new trade deals so the USMCA special secrecy rights become the global standard.[1] But USMCA is currently being renegotiated as part of a mandatory six-year review. This offers a rare opportunity to get these terms removed from USMCA and undermine Big Tech's efforts.

This memo examines important federal and state AI and kids' online safety bills and laws that include transparency and auditing such requirements and, therefore, could be undermined by USMCA source code and algorithm secrecy guarantees. We focus on active federal bills with bipartisan support and policies enacted at the state level and provide excerpts of legal language and explanations of the USMCA conflict to make clear that this problem is real.

1 For background, see: David Dayen, "Big Tech Lobbyists Explain How They Took Over Washington," The American Prospect, April 18, 2023, https://prospect.org/2023/04/18/2023-04-18-big-tech-lobbyists-took-over-washington/; Daniel Rangel and Lori Wallach, International Preemption by "Trade" Agreement: Big Tech's Ploy to Undermine Privacy, AI Accountability, and Anti-Monopoly Policies, Rethink Trade (March 2023), https://rethinktrade.org/reports/international-preemption-by-trade-agreement/.

How International Preemption of Domestic Digital Policy via Trade Agreement Works

In practice, 'trade' rules can be used to undermine public interest policies when a company operating in another country faces regulation it opposes and informs its home government of a potential conflict with 'trade' obligations of the country in which it is operating. After consultations, a trade-agreement enforcement panel could find that the policy violates the agreement and order the country trying to enforce the challenged policy to alter or eliminate the policy or face trade sanctions. Already, U.S. Big Tech firms have gotten the Trump administration to threaten several Canadian digital policies with claims of USMCA 'digital trade' rules violations.

Plus, the 'trade' rules often have a bad effect before any formal dispute is filed: Policymakers may weaken or abandon proposed regulations to avoid potential trade challenges, a phenomenon known as regulatory chill that is a much more common problem with deregulatory trade terms than actual formal challenges.

The ongoing efforts to regulate AI in the European Union provide a real-world example. During the development of the EU Artificial Intelligence Act, European trade officials raised concerns that requirements proposed by the European Commission's Directorate-General for Communications Networks, Content and Technology (DG CONNECT) allowing regulators and auditors to access source code could conflict with source code secrecy provisions in the EU-UK Trade and Cooperation Agreement. That pact unfortunately includes a rule forbidding governments from requiring access to source code for independent audits. The EU domestic AI oversight policies were subsequently narrowed, limiting the circumstances in which regulators and auditors could access source code for high-risk AI systems.[2]

There is also an example of the chilling effect of USMCA's 'digital trade' rules, although it concerns a different provision from the one that limits governments' ability to require the disclosure of source code and algorithms. In February 2026, Mexico's executive branch introduced legislation amending the Federal Labor Law and Federal Copyright Law to establish new rules governing the use of artificial intelligence to reproduce artists' voices and images. The proposal included new consent, contractual, liability, and penalty requirements affecting digital platforms and other companies.[3] The proposal drew criticism from the Mexican Association of Information Technology Industries (AMITI, for its acronym in Spanish), which cited potential conflicts with the USMCA. The industry group focused on Article 19.17, the agreement's 'digital trade' rule that locks in and exports the platform liability shield adopted in the United States through Section 230 of the Communications Decency Act. AMITI argued that the proposed bill could shift liability for users' actions onto digital

2 Luca Bertuzzi, "How Trade Commitments Narrowed EU Rules to Access AI's Source Codes," Euractiv, May 3, 2023, https://www.euractiv.com/news/how-trade-commitments-narrowed-eu-rules-to-access-ais-source-codes; EU-UK Trade and Cooperation Agreement, art. 207.

3 Cámara de Diputados, "Iniciativa del Ejecutivo federal en materia de derechos de las personas trabajadoras artistas intérpretes o ejecutantes," Gaceta Parlamentaria, February 24, 2026.

platforms in a manner forbidden by USMCA Article 19.17. AMITI also warned that moving forward with AI legislation at that time could complicate the upcoming 2026 USMCA review and called for further technical dialogue with lawmakers.[4]

Before the legislation was enacted, the proposal was narrowed. The version approved by Mexico's Chamber of Deputies in April included changes to provisions governing AI-generated voice and image, including new limits on consent and removing certain proposed penalties. The modified legislation was subsequently enacted in May 2026.[5]

What Source Code and Algorithm Secrecy Provisions Actually Do

USMCA Article 19.16 (Source Code) prohibits governments from requiring access to "*a source code of software*" or "*an algorithm expressed in that source code*" as a condition of the import, distribution, sale, or use of software, subject to limited exceptions. **USMCA Article 19.1** defines an algorithm as "*a defined sequence of steps, taken to solve a problem or obtain a result*." By covering both source code and algorithms, and defining the latter so broadly, the USMCA provision could potentially reach descriptions of algorithms, not only the detailed source code developed by programmers.

DOMESTIC POLICY PREEMPTION THROUGH TRADE DEALS IN THE UNITED STATES

The Demise of Beef and Pork Mandatory Country of Origin Labeling (MCOOL)

The United States adopted mandatory country-of-origin labeling requirements for beef and pork, requiring meat marketed as a U.S. product to come exclusively from animals born, raised, and slaughtered in the United States. Canada and Mexico challenged the requirements at the World Trade Organization (WTO), arguing that they constituted an illegal trade barrier under the WTO's Agreement on Technical Barriers to Trade. In 2012, the WTO ruled against the U.S. policy, and after the United States made changes in an attempt to comply, the WTO Appellate Body upheld the finding in 2015 and authorized Canada and Mexico to impose more than $1 billion annually in trade sanctions. Under significant pressure by the Obama administration and industry lobbyists to resolve the dispute, Congress repealed mandatory COOL for beef and pork in 2015 despite the policy enjoying broad bipartisan public support.[6]

4 Asociación Mexicana de la Industria de Tecnologías de Información (AMITI); "AMITI alerta sobre riesgos a la innovación en iniciativa de ley sobre Inteligencia Artificial," April 6, 2026; Rodrigo Riquelme, "Iniciativa sobre inteligencia artificial puede afectar revisión del T-MEC: AMITI," El Economista, April 13, 2026.

5 "Decreto en materia de derechos de las personas trabajadoras artistas intérpretes o ejecutantes," Diario Oficial de la Federación, May 14, 2026.

6 Katie Hettinga and Lori Wallach, "Hamburger Hell: Record High Consumer Beef Prices that Tariffs Haven't Caused, Imports Haven't Lowered, and the Cattle Cycle Can't Explain but that Can Be Fixed," Rethink Trade, 2026, pp. 23–24.

Big Tech lobbyists argue the provision is intended to protect developers' innovations from theft by competitors. Except trade pacts already include 'trade secrets' protections that do just that, but also allow access to technologies, like new medicines, for safety testing. The lobbyists also cynically claim that the second clause of **Article 19.16** provides a broad exception even though it is explicitly drafted with tricky conditions that limit its application. Indeed, the exception in USMCA Article 19.16.2 would not cover the sorts of general disclosure and oversight requirements examined in this memo. The exception applies to source code disclosure requests by regulatory bodies or judicial authorities "*for a **specific** investigation, inspection, examination, enforcement action, or judicial proceeding*" (emphasis added). This narrow exception is predicated on a specific event or investigation already underway, limiting the ability of regulatory bodies to obtain source code or algorithmic information as part of inclusive proactive oversight. Yet regulators may need access to that information in the first place to determine whether a violation has occurred and establish the basis for an investigation.

Current USMCA Renegotiation Offers a Rare Opportunity to Fix This Threat

To date, few other countries have adopted the extreme USMCA limits on proactive external monitoring obligations, even as technology firms' lobbyists are relentlessly pushing the USMCA model worldwide. But lately, the lobbyists are making some headway. That is why eliminating this provision from USMCA has much greater importance than just mitigating its chilling effect in the United States, Canada, and Mexico. Fortunately, the three USMCA countries are now engaged in the renegotiation of the pact in the context of a mandatory six-year joint review. This review provides an opportunity to address digital trade provisions that could constrain domestic regulatory policy. As Congress and state legislatures continue to develop AI safety and kids' online safety regulation, policymakers must ensure that USMCA rules do not restrict the ability of governments to address emerging risks from 21st-century technologies.

Federal AI Regulation Bills Conflicted by the USMCA "Source Code" Rule

S.2938 AI RISK EVALUATION ACT

Summary: Introduced by Sens. Josh Hawley (R-Mo.) and Richard Blumenthal (D-Conn.), this bill would establish an Advanced Artificial Intelligence Evaluation Program within the Department of Energy to assess high-power AI models and mitigate catastrophic risks. The bill requires developers of advanced AI systems trained with massive amounts of computing power to give the Secretary of Energy access to critical information about their models, including model weights, architecture, training data, and underlying code.

CONFLICTS WITH SOURCE CODE AND ALGORITHM SECRECY RULES	RELEVANT PROVISION
The main conflict is with core provisions in **Section 4(a)**, which requires covered developers to participate in the evaluation program and, upon request, provide the Secretary with materials and information necessary to carry out the program. Importantly, the bill states that this information may include the underlying code of the AI system. This creates direct conflict with **USMCA Article 19.16**. The provision's narrow exception in **Article 19.16.2**, which permits a regulatory body to require firms to make source code or algorithmic information available for a "**specific investigation, inspection, examination, enforcement action, or judicial proceeding**," is unlikely to cover this policy. **S. 2938**'s explicit purpose is to authorize the Department of Energy to compel developers of frontier systems to share key algorithmic information with government authorities. Access to the underlying code is expressly contemplated. Thus, the bill's provisions on access to source code and algorithms are neither incidental nor	***Section 4 (a)***: "OBLIGATION TO PARTICIPATE; ENFORCEMENT AND PENALTIES. IN GENERAL.—Each covered advanced artificial intelligence system developer shall— (1) participate in the program; and **(2) provide to the Secretary, on request, materials and information necessary to carry out the program**, which may include, with respect to the advanced artificial intelligence system of the covered advanced artificial intelligence system developer— (A) ***the underlying code of the advanced artificial intelligence system***; (B) data used to train the advanced artificial intelligence system; (C) model weights or other adjustable parameters for the advanced artificial intelligence system; (D) the interface engine or other implementation of the advanced artificial intelligence system; and

contingent on specific investigations or enforcement actions. Rather, the policy's central purpose is to give the government advanced, general access to detailed information from leading AI developers. The compulsory nature of the obligation to provide access to detailed algorithmic information, potentially including source code, is reinforced by **Section 4(b)**, which makes clear that failure to comply with the requirement to participate in the program and provide the information and documentation requested by the authorities would result in a deployment ban.	(E) detailed information regarding the training, model architecture, or other aspects of the advanced artificial intelligence system. **Section 4(b)**: "PROHIBITION ON DEPLOYMENT.—***No person may deploy an advanced artificial intelligence system for use in interstate or foreign commerce unless that person complies with subsection (a)***." (Emphasis added.)
Given that Section **5(a)(3)** contemplates independent third-party assessments and blind model evaluations, this provision also appears to be in conflict with **USMCA Article 19.16**. Regarding the exception in **USMCA Article 19.16.2**, it only exempts access to a "regulatory body." Thus, if the Department of Energy were to facilitate access to source code or detailed algorithmic information to independent third parties, even with safeguards against unauthorized disclosure, such access could potentially violate **USMCA Article 19.16** and would not be covered by the exception included in the second paragraph.	**Section 5(b)(3)**: "ACTIVITIES.—The program shall— (3) To the extent feasible, establish and facilitate classified, independent third-party assessments and blind model evaluations to maintain transparency and reliability."

H.R. 9925 FRONTIER ACT

Summary: Introduced by Reps. Jay Obernolte (R-Cal.) and Lori Trahan (D-Mass.), the Frontier Risk Oversight, National Transparency, Independent Evaluation and Reporting Act (FRONTIER Act) would establish federal oversight over frontier AI models and their developers. It would require frontier developers to register with the Department of Commerce, publish timely risk frameworks, report catastrophic risks, and undergo biannual independent audits. Civil penalties are established for violations, and independent verification organizations are granted limited immunity from suits regarding catastrophic risks.[7]

CONFLICTS WITH SOURCE CODE AND ALGORITHM SECRECY RULES	RELEVANT PROVISION
One of the main potential conflicts between this bill and USMCA's source code and algorithm secrecy guarantees arises from **Section 4** of the bill, titled ***Transparency and Reporting***. This section requires large frontier developers to allow for biannual independent audits by third parties to ensure compliance with self-developed AI frameworks. For auditing purposes, the bill requires developers to provide auditors with access to their unredacted "**materials, systems, and all other information reasonably necessary to comply with its obligations under this subsection**." The term "systems" is broad and not explicitly defined anywhere in the bill. U.S. government enforcers and tech companies could reasonably understand that source code or descriptions of algorithms would fall under the definition of "**systems**." And the catchall clause of "and all other information" would also easily be understood to include detailed descriptions of algorithms and	**Section 4 (c)**: "COMPLIANCE AUDIT.—Not later than one year after the date of enactment of this Act, or 90 days after a developer first qualifies as a large frontier developer, whichever is later, and annually thereafter, ***a large frontier developer shall retain a third party to perform an independent audit of compliance with the frontier AI framework of such developer published pursuant to subsection (a)***. The third party shall conduct the audit consistent with generally accepted auditing approaches, best practices, frameworks, and methods and shall possess demonstrated competence to perform the audit, including experience employing or contracting with individuals who possess technical expertise in the safety of frontier models. A large frontier developer shall not retain a third party if either the developer or the third party has a financial interest in the other. A large frontier developer may compensate a third party for its services but shall not condition any

7 Notably, Section 9, titled Relationship to State Laws, preempts new state laws imposing substantive obligations on AI developers in covered areas. Under Section 9(a), the bill identifies frontier AI risk transparency, third-party auditing and independent verification, and incident reporting as covered subject areas. The preemption of state law has generated backlash from AI safety advocates. Yet the bill's federal requirements could themselves face constraints under USMCA Article 19.16. Section 9(a)(2)(C) specifically contemplates third-party access requirements that may compel developers to provide access to source code and other technical materials. In effect, this creates a potential double layer of AI regulatory constraint: federal law could limit states' ability to regulate AI, while international trade commitments could separately limit the federal government's ability to impose certain AI regulatory requirements.

perhaps source code as well. Insofar as the FRONTIER Act requires AI developers to share with third parties information that could fall under the broad USMCA definition of algorithms and/or share source code, the policy could conflict with **USMCA Article 19.16**.	payment, or the amount of any payment, on the results of the third party's audit. **Section 4 (c) (1)**: ACCESS. —***The third party shall be granted timely access to all materials, records, personnel, systems, and all other information reasonably necessary to comply with its obligations under this subsection***, including all unredacted versions of materials published pursuant to this Act." (Emphasis added.)
Another source of conflict could come from **Section 5**, titled ***Independent Verification***. This section establishes a separate obligation to allow assessments and ongoing monitoring by licensed independent verification organizations (IVOs). Under **Section 5(e)(1)**, very large frontier developers must grant an IVO timely access to unredacted materials, records, personnel, systems, and all other information reasonably necessary to conduct its assessments and ongoing monitoring. As with **Section 4**, the broad reference to "**systems**" and the catchall clause could potentially encompass source code or descriptions of algorithms, thereby bringing this policy into potential conflict with **USMCA Article 19.16**.	**Section 5 (b)**: "Assessment Requirement.—Not later than one year after the date on which the Under Secretary first licenses an IVO with capacity to accept an engagement under this section, or 90 days after a developer first qualifies as a very large frontier developer, whichever is later, ***a very large frontier developer shall retain an independent verification organization that has been licensed pursuant to the regulations prescribed under subsection (c) of section 3 to perform ongoing assessment of the adequacy of the very large frontier developer's frontier AI framework, governance policies and practices, risk-monitoring, and mitigation of detected risks for achieving acceptable levels of catastrophic risk mitigation***. All assessment, monitoring, reporting, and corrective action obligations under this section shall apply to catastrophic risks arising from a very large frontier developer's internal use of frontier models, in addition to catastrophic risks arising from the release of such frontier models for use by third parties." **Section 5 (e) (1)**: "ACCESS.— (1) IN GENERAL.— ***A very large frontier developer shall grant an IVO timely access upon request to unredacted materials, records, personnel, systems, and all other information reasonably necessary for conducting the assessments and ongoing monitoring required by this section.***" (Emphasis added.)

Federal Kids' Online Safety Bills

S.1748/H.R. 6484
KIDS ONLINE SAFETY ACT (KOSA)

Summary: Introduced by Sens. Marsha Blackburn (R-Tenn.) and Richard Blumenthal (D-Conn.) in the Senate and Rep. Gus Bilirakis (R-Fla.) in the House (Representative Kathy Castor (D-Fla.) co-led the House version in the 118th Congress), KOSA would establish federal safety requirements for online platforms used by minors. The bill would impose a duty of care on covered platforms, require safeguards and parental controls, establish transparency and disclosure requirements, and require certain platforms to undergo independent third-party audits.[8]

CONFLICTS WITH SOURCE CODE AND ALGORITHM SECRECY RULES	RELEVANT PROVISION
Section 105 (e), ***Transparency***, requires covered platforms to undergo independent third-party audits and to provide all relevant information and materials to auditors for that process, as well as access to "all network, systems, and assets" relevant to the audit. Similar to the ***FRONTIER Act***, the term "systems" is not defined in the bill. U.S. government enforcers and tech companies could reasonably understand the broad use of "systems" to include underlying software's algorithms and source code. Thus, this provision likely conflicts with **USMCA Article 19.16**.	**Section 105 (e)**: "COOPERATION WITH INDEPENDENT, THIRD-PARTY AUDIT.—To facilitate the report required by subsection (c), a covered platform shall— 1) ***provide or otherwise make available to the independent third-party conducting the audit all information and material in its possession, custody, or control that is relevant to the audit***; (2) provide or otherwise make available to the independent third-party conducting the audit access to ***all network, systems, and assets*** relevant to the audit" (emphasis added).

8 The House incorporated a revised version of KOSA into H.R. 7757, the KIDS Act, which passed on June 29, 2026. The House version omits the Senate bill's duty-of-care provision and includes a broad state preemption provision similar to the one found in the FRONTIER Act. The House version retains the same audit and auditor-access requirements that conflict with USMCA Article 19.16.

ILLINOIS SB 0315: ARTIFICIAL INTELLIGENCE SAFETY MEASURES ACT

Summary: Enacted by the Illinois General Assembly in 2026 and effective January 1, 2027, SB 0315, the Artificial Intelligence Safety Measures Act, establishes requirements for large frontier AI developers. The law requires developers to establish and publish a frontier AI framework for managing catastrophic risks associated with their models and undergo annual independent third-party audits of compliance. It also establishes transparency and reporting requirements for frontier AI developers, including requirements to report certain safety incidents and assessments of catastrophic risk.

CONFLICTS WITH SOURCE CODE AND ALGORITHM SECRECY RULES	RELEVANT PROVISION
The main issue of conflict, similar to the **FRONTIER Act**, is the broad scope of information an independent auditor may need to conduct its audit and to which an AI developer is required to grant access. **Section 10(d)(1)** requires large frontier developers to grant auditors access to "**all materials reasonably necessary**" to conduct their audits, but it does not define the scope of that requirement or expressly exclude source code or algorithmic information. This could create a conflict with **USMCA Article 19.16**, since auditors are likely to determine that access to source code, or at least detailed descriptions of the algorithms powering a frontier AI model, is necessary to assess a developer's compliance with the Act. Additionally, because these would be recurring compliance audits rather than specific investigations or enforcement actions, the exception in **Article 19.16.2** would not apply. The bill does provide protection for sensitive information by allowing developers to impose security and confidentiality protocols	**Section 10(d)**: "Beginning on January 1, 2028 or 90 days after a developer first qualifies as a large frontier developer, whichever is later, ***a large frontier developer shall annually retain a third party to perform an independent audit*** of compliance with the requirements of this Section." **Section 10(d)(1)**: "The third party shall be granted ***access to all materials reasonably necessary*** to comply with the third party's obligations under this subsection (d), including, but not limited to, all unredacted versions of materials published pursuant to this Act. To protect the frontier developer's trade secrets and confidential business information, cybersecurity, national security of the United States, or public safety, a large frontier developer may impose security protocols on the third party, including, but not limited to, restrictions on note taking, copying, retaining, or removing materials; requirements for on-premise review; and

on auditors, but these protections govern how information is accessed and handled rather than excluding source code or algorithmic information from the audit requirement.	confidentiality requirements." (Emphasis added.)

CALIFORNIA SB 1119: ADAM'S LAW

Summary: Enacted by the California Legislature in 2026, SB 1119, Adam's Law, establishes requirements for operators of companion chatbots to protect children. The law requires operators to conduct and document comprehensive child safety risk assessments and undergo initial and recurring independent child safety audits. An additional audit is required before a substantially modified companion chatbot is made publicly available if a risk assessment finds that the modification would increase child safety risks. It also establishes reporting and recordkeeping requirements related to these audits, including requirements to report audit findings to the Attorney General and publish summaries of audit results.

CONFLICTS WITH SOURCE CODE AND ALGORITHM SECRECY RULES	RELEVANT PROVISION
Similar to the **FRONTIER Act** and Illinois **SB 0315**, the main conflict between this law and USMCA's source code and algorithm secrecy guarantees is the broad scope of information an independent auditor may need to conduct its audit. **Section 21814(a)(3)(A)** requires operators to grant auditors access to "**all documentation reasonably necessary**" to comply with their audit obligations, but it does not define the scope of that requirement or expressly exclude source code or algorithmic information. This could create a conflict with **USMCA Article 19.16**, since an auditor could determine that access to source code, or at least detailed descriptions of the algorithms powering a companion chatbot, is necessary to assess whether the operator has complied with the law's child safety requirements. Additionally, **Section 21814(a)(1)(A)(ii)** requires	**Section 21814(a)(1)(A)(ii)**: "After an initial child safety audit is performed, the operator shall ensure the performance of an ***independent child safety audit of a companion chatbot every two years thereafter***, except that the operator shall ensure that a child safety audit is performed before a substantial modification to the companion chatbot for which the applicable risk assessment shows an increased child safety risk is made publicly available." **Section 21814(a)(3)(A)**: "An auditor shall be ***granted access to all documentation reasonably necessary*** to comply with the auditor's obligations under this subdivision. The operator shall retain this documentation for as long as the companion chatbot is deployed plus five years."

independent child safety audits every two years, meaning these are recurring compliance audits rather than specific investigations or enforcement actions, so the exception in **Article 19.16.2** would not apply. The bill does provide protection for sensitive information by allowing operators to impose security and confidentiality protocols on auditors, but these protections govern how information is accessed and handled rather than excluding source code or algorithmic information from the audit requirement.	**Section 21814(a)(3)(B):** "To protect the operator's trade secrets and confidential business information, cybersecurity, individual privacy, or public safety, an operator may impose security protocols on the auditor, including, but not limited to, restrictions on note taking, copying, retaining, or removing materials, requirements for on-premise review, and confidentiality requirements." (Emphasis added.)

TEXAS HB 18: SECURING CHILDREN ONLINE THROUGH PARENTAL EMPOWERMENT (SCOPE) ACT

Summary: Enacted by the Texas legislature in 2023 and effective primarily beginning in 2024, HB 18, the Securing Children Online through Parental Empowerment (SCOPE) Act, establishes requirements for digital service providers that offer services to minors. The law requires providers to obtain parental consent and limit the collection and use of minors' personal information and targeted advertising. It also requires providers to implement parental tools and safeguards against harmful content. The law establishes requirements governing how digital service providers use algorithms in connection with minors and provides enforcement authority to the Texas attorney general and a private right of action for parents or guardians.

CONFLICTS WITH SOURCE CODE AND ALGORITHM SECRECY RULES	RELEVANT PROVISION
The main conflict with USMCA source code and algorithm secrecy guarantees is in **Section 509.053(b)(1)(G)**. This section requires digital service providers to make their "**algorithm code**" available to independent security researchers as part of their strategy to prevent minors from being exposed to harmful material. "Algorithm code" clearly falls within the scope of information to which **USMCA Article 19.16**	**Section. 509.053**: "DIGITAL SERVICE PROVIDER DUTY TO PREVENT HARM TO KNOWN MINORS. (a) In relation to a known minor's use of a digital service, a digital service provider shall develop and implement a strategy to prevent the known minor's exposure to harmfulmaterial and other content that promotes, glorifies, or facilitates: (1) suicide,

forbids government officials from requiring companies to provide access. **Section 509.058** provides an exception for trade secrets, meaning a provider does not have to disclose information that qualifies as a trade secret. However, this does not resolve the conflict with **Article 19.16**, since even code that does not qualify as a trade secret would still be covered by the source code and algorithm secrecy guarantees in USMCA.	self-harm, or eating disorders; (2) substance abuse; (3) stalking, bullying, or harassment; or (4) grooming, trafficking, child pornography, or other sexual exploitation or abuse. (b) A strategy developed under Subsection (a): (1) must include: (A) creating and maintaining a comprehensive list of harmful material or other content described by Subsection (a) to block from display to a known minor; (B) using filtering technology and other protocols to enforce the blocking of material or content on the list under Paragraph (A); (…) (G) ***except as provided by Section 509.058, making available the digital service provider's algorithm code to independent security researchers***; (…)" (emphasis added).
A second provision that could conflict with **USMCA Article 19.16** is **Section 509.056**, which requires certain digital service providers to disclose an overview of how their algorithms provide, promote, rank, or filter information, as well as the personal identifying information used as inputs. While this section does not expressly require access to source code, its algorithmic disclosure requirements could be captured under the broader protections for algorithms under **USMCA Article 19.16**.	**Section. 509.056**: "USE OF ALGORITHMS. A digital service provider that uses algorithms to automate the suggestion, promotion, or ranking of information to known minors on the digital service shall: (1) make a commercially reasonable effort to ensure that the algorithm does not interfere with the digital service provider's duties under Section 509.053; and (2) ***disclose in the digital service provider's terms of service, privacy policy, or similar document, in a clear and accessible manner, an overview of:*** (A) the manner in which the digital service uses algorithms to provide information or content; (B) ***the manner in which algorithms promote, rank, or filter information or content; and (C) the personal identifying information used as inputs to provide information or content.***" (Emphasis added.)

Conclusion

The bills and laws examined in this memo reflect a growing effort by Congress and state legislatures to establish meaningful transparency, accountability, and oversight for AI and children's online safety. Yet the 'digital trade' rules embedded in USMCA Chapter 19 undermine these efforts by limiting governments' ability to require access to source code, algorithms, and other information needed to effectively oversee AI and social media platforms. **USMCA Article 19.16** is particularly concerning because it provides a largely overlooked avenue for challenging laws and regulations that seek greater transparency and accountability from technology companies.

As the USMCA undergoes its first joint review, policymakers have a golden opportunity to reconsider USMCA 'digital trade' rules that could constrain the ability of governments to enact laws addressing emerging technologies. Using the USMCA mandatory six-year review to eliminate the dangerous and unnecessary "Source Code" provisions that Big Tech lobbyists inserted into the USMCA would also signal to countries worldwide not to concede to Big Tech pressure to adopt such terms. It is critical these rules do not become the model for future trade agreements, including large global or plurilateral ones the United States may eventually join, if governments are to retain the ability to make and enforce their own laws in the public interest.

AMERICAN ECONOMIC LIBERTIES PROJECT

rethink TRADE

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

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

economicliberties.us
@econliberties
info@economicliberties.us

rethinktrade.org
@rethinktrade
info@rethinktrade.org