

Big Tech's "Digital Trade" Agenda Threatens South Carolina's Tech Policy Goals

Nationwide, state legislators have introduced bills to protect people from biased artificial intelligence (AI) models, online privacy violations, abuses of children and teens' data, and anti-competitive practices by tech companies—and to guarantee our right to repair our phones, cars and other equipment.

The surge in statehouse tech legislation shows that the American people—and their elected officials at every level—want action now. But few people realize that the very firms whose conduct led to this bipartisan response have a strategy to undermine tech regulation through a stealthy form of international preemption. They want to add rules to international trade deals that limit how state and federal governments can regulate tech.



The most extreme of what these Big Tech interests misleadingly call "digital trade" rules would:

- limit governments' powers to require impact assessments, bias audits, or pre-deployment testing of even high-risk AI and other programs if this involves government regulators or independent reviewers having access to detailed descriptions of algorithms or to source code;
- forbid right to repair policies that require manufacturers to share repair tools that depend on access to code or algorithms;
- ban regulation of international data transfers, guaranteeing rights for firms to choose where our personal data moves and is stored; and
- prohibit requirements to keep certain data locally stored, for instance to keep sensitive data within the state for privacy or any other reason.

South Carolina lawmakers' initiatives to regulate the tech industry must not be thwarted by the "digital trade" rules being pushed by Big Tech firms. We must ensure that South Carolina tech bills are not undermined by this international preemption plot.

The rest of this explainer details how "digital trade" provisions conflict with specific South Carolina policies relating to AI regulation and kids' online safety.



**For a detailed analysis of these "digital trade" rules, see <https://rethinktrade.org/reports/international-preemption-by-trade-agreement/>*

AI REGULATION

To try to avoid civil rights and liberties violations and other harms from AI systems being rushed into use, legislators are introducing bills in statehouses nationwide that require impact assessments, bias audits, or pre-deployment testing to ensure that AI models are fair and accurate. The Big Tech-demanded “digital trade” rule that bans access to source code and algorithms would forbid such reviews from being conducted by or made available to government regulators or independent bodies, as many bills require.

For instance, in South Carolina, HB 4696 (2023) proposed requirements for employers to share information about their use of automated decision systems with employees:

“(g) Impact assessment of automated decision systems. (1) Prior to utilizing an automated decision system, an employer shall create a written impact assessment of the system that includes, at a minimum: (A) a detailed description of the automated decision system and its purpose; (...) (2) An employer shall provide a copy of the assessment prepared pursuant to subdivision (1) of this subsection (g) to an employee upon request.”

By requiring firms to conduct impact assessments of their systems and allowing employees to request them, this proposed policy could be challenged based on algorithm and source code secrecy rules.

KIDS’ ONLINE SAFETY

Source code and algorithms are not AI-specific terms. They also are at the heart of social media, which is another software subject to state-level regulation. If the “digital trade” rules Big Tech seeks were widely enacted, the same “digital trade” secrecy guarantees that forbid regulators’ access to algorithmic information would undermine bills aimed at protecting children from harmful social media models.

The South Carolina’s Age-Appropriate Design Code Act was considered in the 2024 legislative session. This bill establishes requirements for data protection impact assessments, which must include information about algorithmic design:

“(B) A data protection impact assessment required by this section must (...) determine whether the online service, product, or feature is designed and offered in an age-appropriate manner consistent with the best interests of children that are reasonably likely to access the online product by examining at least the following: (...) (4) whether algorithms used by the product, service, or feature could harm children or would result in: reasonably foreseeable and material physical or financial harm to the child; reasonably foreseeable and severe psychological or emotional harm to the child; a highly offensive intrusion on the reasonable privacy expectations of the child; or discrimination against the child based upon race, color, religion, national origin, disability, sex, or sexual orientation; (...) (4) within five business days of a written request by the Attorney General, provide the Attorney General with a copy of any data protection impact assessment.”

The Code requires businesses to complete data protection impact assessments, which shall include “whether algorithms used by the online product, service, or feature could harm children.” Since the state’s Attorney General can demand access to the data protection impact assessments, companies could argue that the law requires them to disclose their algorithms in violation of source code secrecy rules.

The good news is that very few of the hundreds of trade agreements in effect worldwide include Big Tech’s “digital trade” rules. The bad news is that Big Tech lobbyists are using their power and money to try to rig numerous trade deals that are being negotiated right now to derail the wave of tech regulation underway nationwide. To learn more, please visit: www.rethinktrade.org