U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

March 1, 2023

The Honorable Gus Bilirakis
Chair
Subcommittee on Innovation, Data & Commerce
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Innovation, Data & Commerce
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky:

In advance of your Subcommittee's hearing entitled "Promoting U.S. Innovation and Individual Liberty Through a National Standard for Data Privacy," the U.S. Chamber of Commerce reiterates our support for a preemptive privacy standard that protects all Americans equally.

A Single National Privacy Standard

For the United States to continue to reap the benefits of the 21st century digital economy and enable a thriving ecosystem that facilitates small business growth, Congress must pass a single *preemptive* national privacy standard. Simply adopting a national privacy law without strong preemption would enable a state patchwork of laws that will be confusing to both consumers and potentially impossible for small businesses to comply.

A recent report from ITI highlighted that a national patchwork of privacy laws would cost the United States economy $1 trillion and disproportionately impact small businesses with a $200 billion economic burden.[1]

To provide the strongest preemption, according to a Congressional Research Service report, Congress should use words like preemption "related to" certain subjects.[2]

Congress should avoid merely preempting what a proposed bill is "covering" or "covered by," because such clauses are considered by the Supreme Court to be less restrictive on states than phrases like "related to."[3] According to the Supreme Court, "'Covering' is a more restrictive term which indicates that preemption will lie only if the federal regulations substantially subsume the subject matter of the relevant state law."[4] A national privacy law that merely preempts what is "covers" and then provides for exceptions to that preemption would likely be taken by many as evidence that Congress has not intended to "substantially subsume" regulation.

[1] https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/.
[2] https://crsreports.congress.gov/product/pdf/R/R45825
[3] *Id.* at 10.
[4] *CSX Transportation, Inc. v. Easterwood*, 507 U.S. 663 (1993.)

In recent years, legislation has been authored by Republican and Democrats that would provide strong preemption:

- In the 117th Congress, H.R. 1816, the Information Transparency and Personal Data Control Act provided that, "No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard *related to* the data privacy or associated activities of covered entities."[5]
- Also in the 117th Congress, Rep. Armstrong proposed an amendment to the American Data Privacy and Protection Act that would have provided, "No law, rule, regulation, requirement, prohibition, standard, or other provision having the force and effect of law *relating to* any subject matter regulated under this Act…"[6]
- In the 118th Congress, House Financial Services Committee Chairman Patrick McHenry has proposed the "Data Privacy Act of 2023," which provides that legislation "supersedes any statute or rule of a State."[7]

Balanced Enforcement

Compliance should be collaborative and reside with appropriate regulators and enforcers like the Federal Trade Commission (FTC) and state attorneys general and not the trial bar through the use of private rights of action.[8]

Agency Enforcement

FTC has historically been the agency with the expertise in data privacy matters in the federal government for companies not regulated by sectoral data protection laws. The Chamber believes that FTC remains the appropriate agency to continue to regulate and enforce data protection—but with appropriate guardrails.

In light of FTC Commissioner Christine Wilson's recent resignation in protest, the Chamber has called for oversight of the Commission's mismanagement and called for a moratorium on granting the agency further rulemaking authority until appropriate safeguards were placed upon the agency to protect due process.[9]

In particular, we call to your attention FTC's recent Advanced Notice of Proposed Rulemaking in which it appears to replace Congress and develop comprehensive privacy rules. Former Commissioner Noah Phillips who dissented against the proposal stated what the privacy

[5] https://www.congress.gov/bill/117th-congress/house-bill/1816/text (emphasis added)
[6] https://docs.house.gov/meetings/IF/IF17/20220623/114958/BILLS-117-8152-A000370-Amdt-6.pdf (emphasis added).
[7] https://financialservices.house.gov/uploadedfiles/glb_2023_xml_2.24_934.pdf
[8] https://www.uschamber.com/assets/archived/images/9.6.18_us_chamber_-_ctec_privacy_principles.pdf
[9] https://www.uschamber.com/assets/documents/230216_FTC-Oversight_Sen.-CST-House-EC.pdf

rulemaking "does accomplish is to recast the Commission as a legislature, with virtually limitless rulemaking authority where personal data are concerned."[10]

We believe FTC's actions to exceed its authority run afoul of the Supreme Court's "Major Questions Doctrine," which holds that in matters of "political and economic significance" Congress must grant clear authority to an agency to regulate.[11]

The Commission is subject to rulemaking requirements under the Magnuson-Moss Act regarding its mandate to enforce against "unfair and deceptive trade practices."[12] The Magnuson Moss Act did not delegate authority to the FTC but imposed heightened procedural safeguards on the agency. Knowing the FTC is flouting the procedural constraints placed upon it, Congress should not delegate broad new rulemaking authority to the Federal Trade Commission.

For example, Congress should refrain from granting the Commission Administrative Procedure Act-style rulemaking authority to broadly define types of data that are prohibited from collection without exceptions like consumer consent. If the Commission were to determine that broad categories of data are prohibited from collection it would be harmful to small businesses. According to a recent report from the Chamber, **80 percent** of small businesses stated that technology platforms like payments apps, digital advertising, and delivery help them compete with larger companies.[13] **80 percent** of small business also say that limiting access to data will harm their business operations.[14] One small business owner of a coffee shop stated in response to the FTC being able to have this kind of authority said[15]:

> *This is very unfortunate as it would essentially be another "pandemic" for us.* Not having customer data means that we would go back to the early 1980's where we would market our products to a generic list, which in turn would be extremely costly and not a good customer experience. Having customer data helps us customize our marketing so the end result is more meaningful to the customer.

The Commission should narrowly tailer rulemaking authorities that it gives the Federal Trade Commission.

Private Rights of Action

---

[10] https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Phillips%20Dissent%20to%20Commercial%20Surveillance%20ANPR%2008112022.pdf

[11] https://www.uschamber.com/assets/documents/221121_Comments_CommercialSurveillanceDataSecurity_FTC.pdf

[12] 15 U.S.C. § 45.

[13] https://americaninnovators.com/wp-content/uploads/2022/08/Empowering-Small-Business-The-Impact-of-Technology-on-U.S.-Small-Business.pdf

[14] *Id*.

[15] https://www.uschamber.com/technology/small-business-owners-credit-technology-platforms-as-a-lifeline-for-their-business (emphasis added).

Comprehensive privacy legislation should leave enforcement to agencies like the Federal Trade Commission and state attorneys general and not empower the private trial bar at the expense of business innovation and viability. Frivolous, non-harm-based litigation in particular has been used in the past to extract costly settlements from companies, even small businesses, based on privacy law provisions granting a private right of action. Private rights of action are ill-suited in privacy laws because:[16]

- Private rights of action undermine appropriate agency enforcement and allow plaintiffs' lawyers to set policy nationwide, rather than allowing expert regulators to shape and balance policy and protections. By contrast, statutes enforced exclusively by agencies are appropriately guided by experts in the field who can be expected to understand the complexities of encouraging compliance and innovation while preventing and remediating harms.
- They can also lead to a series of inconsistent and dramatically varied, district-by-district court rulings. Agency enforcement can provide constructive, consistent decisions that shape privacy protections for all American consumers and provide structure for companies aiming to align their practices with existing and developing law.
- Combined with the power handed to the plaintiffs' bar in Federal Rule of Civil Procedure 23, private rights of action are routinely abused by plaintiffs' attorneys, leading to grossly expensive litigation and staggeringly high settlements that disproportionally benefit plaintiffs' lawyers rather than individuals whose privacy interests may have been infringed.
- They also hinder innovation and consumer choice by threatening companies with frivolous, excessive, and expensive litigation, particularly if those companies are at the forefront of transformative new technologies.

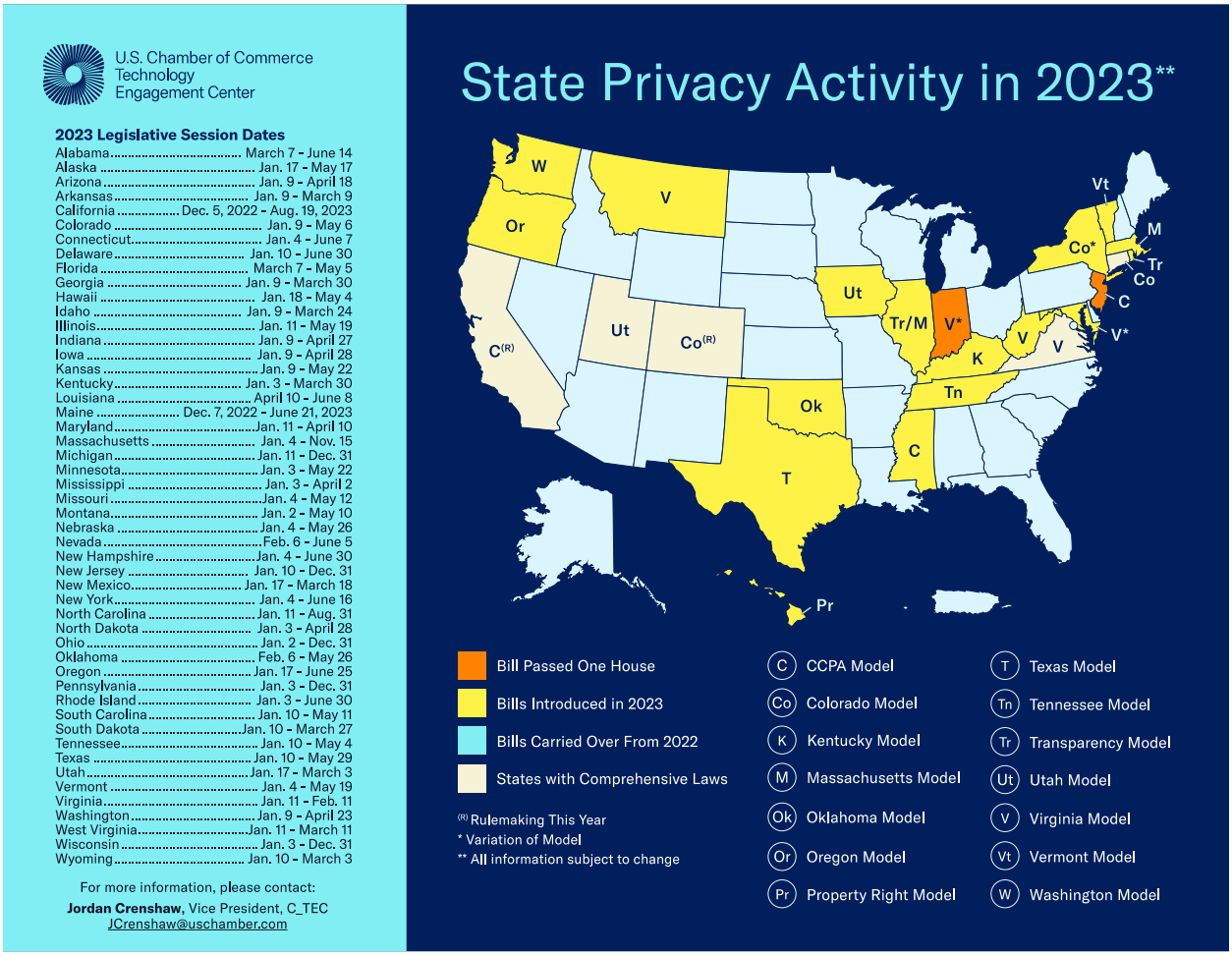
Private rights of action would be particularly devastating for business under a privacy law that does not have a strong preemptive effect. Not only would states be able to continue passing their own laws, but individual judicial district precedent could also create further confusion and conflict.

Harmonizing State Trends

Congress should incorporate principles from good state legislation into a national privacy law because companies are already operationalizing requirements in five states. It has been more than 1,700 days since the California Consumer Privacy Act (CCPA) was signed into law. Since then, four other states have passed comprehensive privacy laws and another 20 are considering their own bills. The map provided below[17] illustrates that states are looking at diverging privacy proposals which further emphasizes the need for a preemptive national privacy standard.

[16] https://instituteforlegalreform.com/wp-content/uploads/2020/10/Ill-Suited_-_Private_RIghts_of_Action_and_Privacy_Claims_Report.pdf

[17] For detailed summaries of the state proposals visit https://americaninnovators.com/2023-data-privacy/.



When framing a national privacy law, Congress should assess where trends are developing. For example, all state privacy laws that have been enacted provide some form of transparency requirement and grant consumers access, deletion, correction, and opt out rights in the case of things like data sales. No state privacy law has created a private right of action for privacy violations. Rather, these laws have granted state attorneys general or other relevant agencies enforcement powers. No state privacy law has strict opt-in or broad data collection prohibitions that as described above could harm small businesses. As a general trend, red and purple states like Texas, Indiana, Maryland, Iowa, and Montana are considering legislation that resemble variants of Virginia's new privacy law. Traditionally blue states are considering legislation that resembles either CCPA, the American Data Privacy and Protection Act, or strictly opt-in consent regimes with private rights of action.

Conclusion

It is urgent that Congress pass preemptive national privacy legislation that provides strong protections for all Americans equally. Additionally, agencies like the FTC should be given narrow

grants of authority with appropriate guardrails. Enforcement should not be exercised through private rights of action. We also urge Congress to build operational harmony into a national privacy law by drawing upon workable provisions of state privacy laws that protect consumers and provide certainty.

Sincerely,

Jordan Crenshaw
Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce

cc: House Energy & Commerce Committee