

[DATA PRIVACY]



A Federal Data Privacy Legislative Framework

Bipartisan Recommendations on Preemption,
Enforcement, and Private Right of Action for
Legislators and Policymakers



NTSC
NATIONAL TECHNOLOGY
SECURITY COALITION

ntsc.org



An effective and meaningful approach toward data privacy requires a single comprehensive bill.

When legislators approach the issue of protecting sensitive personal data, two main considerations emerge. First, the steady pace of cyberattacks compromises both valuable intellectual property and millions of records that include personally identifiable information (PII). Second, consumers grow increasingly concerned about how companies use data collected about them. The EU's General Data Protection Regulation (GDPR), which came into effect in May 2018, is the most prominent example of the global rise of regulatory frameworks focused on data security and protection, use, and privacy. In the United States, with the California Consumer Privacy Act (CCPA) becoming effective in January 2020 and other states continuing to introduce data privacy and protection legislation, businesses across the country will soon be faced with more and more conflicting regulations.

An effective and meaningful approach toward data privacy requires a single comprehensive bill—avoiding a flurry of contradictory state laws—that addresses how we define and protect sensitive personal data and deidentified data, establishes minimum standards of protection and care, and outlines uniform rules governing data protection, security, breach notification, and regulatory oversight. Unitary regulations would ensure that citizens have equal protection wherever they reside or wherever their data is stored while avoiding a myriad of disparate rules and regulations that add complexity and undue costs.

Three Key Obstacles Preventing The Passing of a Federal Privacy Law

Congress has introduced several federal data privacy bills within the last year, with both parties productively engaging in dialogue and discussion. During the course of these negotiations, it's become clear where the political parties need to collaborate and, where necessary, compromise for a federal data protection and privacy bill to succeed.

Here are the three key obstacles, the NTSC's position, and a pragmatic suggestion for compromise that will please both parties.

PREEMPTION

Generally, the Republicans support preemption as a part of any federal mandate while Democrats mostly oppose it. Digging deeper, the issue is more nuanced on the Democratic side. At a high level, they fear a federal privacy law without preemption will weaken strong state privacy laws. However, some Democrats have suggested that preemption may be an option if the federal solution is as strong as the strongest state privacy laws. This opening leaves room for a compromise if Republicans are willing to base a federal privacy law on the strongest state privacy law (such as the CCPA).

Why is preemption so important? Republicans staunchly support preemption out of a recognition that we do not want to go down the same road as data breach notification laws. If we look at current state privacy laws, we note:



Three states (California, Maine, and Nevada) have already passed laws with varying strictness. These three laws vary in comprehensiveness, with California's as the strictest and Nevada's as the weakest. Already, consumers are protected unequally in three different states.



15 states have pending laws in progress: Like the three passed state laws, these 15 bills are inconsistent in requirements and severity—ranging from the stricter-than-CCPA New York Privacy Act to the much less strict Nebraska Consumer Data Privacy Act.



Many bills have died: Agreement upon data privacy law principles, even within states, is fraught with sticking points that kill bills. In some cases, like Wisconsin, three attempts have led to nothing so far.

Across the states, fundamental elements including the definition of what comprises sensitive data and deidentified data along with rights such as right of data access, rectification, deletion, restriction, portability, and opt-out are inconsistent and vary from bill to bill. This means consumer privacy rights vary from state to state. This situation drives the argument for preemption.

Consumer privacy rights vary from state to state—this drives the argument for preemption.



A federal data privacy bill should align with, recognize, and leverage existing federal data privacy and security laws.

NTSC Position on Preemption

As a purely practical matter, there is absolutely no benefit to businesses, consumers, or regulators in promulgating a federal privacy framework that establishes a baseline but does not preempt competing state and local privacy frameworks such as the California Consumer Privacy Act (CCPA). Absent preemption, states will inevitably create varying requirements and impose additional, different, and/or more stringent privacy requirements, with the result that the patchwork of disparate privacy laws across the U.S. will expand and businesses will have to comply with divergent and potentially inconsistent requirements—diverting scarce resources away from improving data protection for consumers.

That patchwork means that businesses will not have predictability and consumers may experience differential treatment depending upon where they reside and/or where their data was impacted. In addition, the absence of a preemptive national privacy framework complicates international issues of interoperability and essentially renders U.S. federal privacy practices meaningless in terms of a global approach to data protection and privacy risk management.

To the degree practicable, a federal data privacy bill should align with, recognize, and leverage existing federal data privacy and security laws such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and other sector-specific laws. With rare exceptions, we do not support the preemption of other federal data privacy and security laws.

NTSC Recommendation on a Preemption Compromise

In terms of preemption, three recommendations may make a bill more palatable to advocates for state privacy laws:



Giving limited enforcement rights to authorized state regulators and enforcement officials.



Creating a centralized repository of privacy-related reports and information that is accessible to authorized federal and state regulators and enforcement officials for law enforcement purposes, similar to the FTC's current Consumer Sentinel consumer complaint database.



To the extent that a bill doesn't also preempt other existing federal privacy frameworks (e.g. education, finance, health, communications, children) in favor of a single approach (i.e. similar to GDPR's single framework), include **a provision requiring federal entities to consult, coordinate, and develop harmonizing principles** to preclude a federal patchwork of inconsistent privacy law and enforcement practices.

ENFORCEMENT

This second sticking point has a high chance of successful compromise between Republicans and Democrats compared to preemption and a private right of action. Both parties agree that the FTC should enforce a federal data privacy law. Disagreements exist around the scope of the FTC's enforcement and the role of state attorneys general.

Republicans are comfortable with the FTC handling enforcement, with some caveats. For example, Republicans want to define "reasonable security measures" and not grant the FTC rulemaking authority or the ability to fine a covered entity for the first instance of a breach. Democrats' thoughts on enforcement are more mixed—ranging from the FTC handling everything with rulemaking authority and fining covered entities for the first instance of a breach to a separate enforcement agency within the FTC with approximately 500 employees all focused on enforcing the federal mandate when a violation occurs.

NTSC Position on Enforcement

The NTSC supports recognizing and leveraging existing federal data privacy regulators. Several groups have also discussed the notion of providing state attorneys general with enforcement rights under a federal privacy law. Children's Online Privacy Protection Act (COPPA) is a good model to use for reference because it has preemption, states and state attorneys general are familiar with its enforcement approach, and the language is fairly typical for statutes in which the FTC (referred to as "Commission" in COPPA) has primary authority but states (and sometimes other federal entities) have shared enforcement rights as well. Such an arrangement prohibits a regime where 50 different interpretations of a federal data privacy law is possible.

NTSC Recommendation on an Enforcement Compromise

The FTC and states have a long history of joint consumer protection enforcement activities and federal/state task forces, which presumably would help both federal and state authorities leverage their scarce privacy resources. Under the COPPA model, states would get access to federal jurisdiction, venue, and service of process provisions, which typically are broader than states' rights would be under their own state law, and direct access to federal district courts. And while they would need to keep the FTC in the loop, this approach would preclude the need (and costs) for a separate Privacy Bureau, negate the concerns for funding such a bureau, and would perhaps help to avoid the proliferation of state privacy laws.



This second sticking point has a high chance of successful compromise between Republicans and Democrats.

Any federal privacy framework should focus on actual harms and real risk of injury to individuals rather than on hypothetical harms or technical violations of the statute.

PRIVATE RIGHT OF ACTION

This issue is the simplest and toughest point of contention. Republicans want to exclude a private right of action while Democrats support a private right of action. Excluding a private right of action is justified on the basis of helping businesses avoid getting hit with frivolous lawsuits. If a federal privacy law is sufficiently strict (e.g. equal to the CCPA), then the accountability and reporting requirements—along with FTC enforcement—will be sufficient to “punish” a business without needing to add individual lawsuits. Some moderate Democrats may not support a private right of action.

However, many Democrats support a private right of action because they feel a consumer should be able to individually sue a company in case other punitive recourses are not sufficient. This position stems from a general distrust that businesses and enforcement agencies like the FTC will not adequately protect consumers. Thus, the argument goes, consumers need their own recourse to sue in case other legal machinery fails them.

NTSC Position on Private Right of Action

Any federal privacy framework should focus on actual harms and real risk

NTSC Recommendation on a Private Right of Action Compromise

Those more technical areas of noncompliance would remain within the exclusive purview of federal and state regulators and enforcers, who are in a better position to determine the associated risk and enforce compliance to the extent deemed necessary.



8 ELEMENTS NEEDED IN A FEDERAL DATA PRIVACY BILL

The following items would allow for compromise across the aisle in Congress, eliminate key sticking points, and ensure unitary, consistent, and comprehensive requirements.

- **Preempt state and local privacy laws:** As discussed, selecting the highest state standard as a benchmark can win over the objections of Democrats who fear preemption would weaken existing state data privacy standards.
- **Consistent enforcement authority:** It seems likely the FTC will enforce this law (as agreed upon by Republicans and Democrats), and this enforcement needs to be consistent—not leaving room for arbitrary and inconsistent FTC interpretations.
- **No private right of action:** Democrats can be reassured by a federal data privacy law with high, specific standards that is well-enforced. As mentioned earlier, private right of action can still exist in limited situations involving harm arising from actual data breaches.
- **An unambiguous definition of personal and deidentified data** that comprises “covered information” under the law: It’s important not to leave these definitions vague in a federal data privacy law.
- **Consistent civil penalty judgments:** Irregularity in civil penalty judgments leads to inconsistent application of the law and leaves room to arbitrarily punish some companies over others.
- **Interoperability with other industry-specific federal privacy and data protection laws and globally recognized regulatory regimes** such as the European Union General Data Protection Regulation (GDPR): Regulatory interoperability is important not only for companies that must already adhere to data privacy requirements already existing as a part of industry-specific laws (such as HIPAA or GLB) but also for global commerce (especially when negotiating trade deals).
- **Practical regulations covering the timing and extent of breach notification:** If breach notification regulations are unrealistic and unpragmatic, then they will not be followed—defeating the purpose of a federal data privacy law. (Ideally, a federal data privacy bill may also want to address national data breach notification requirements, or a separate national data breach notification law can get passed that is consistent with a companion federal data privacy law). A bill must be careful that the definition of breach is not overbroad, which would likely lead to regulators being inundated with breach notification claims based solely on mere “access” where no exfiltration took place, no harm was caused, and the consumer was not put at risk.
- **Unambiguous accountability and reporting requirements:** Again, specificity and consistency is key so that companies are all held to the same standard (with variations depending upon industry and type of information to be protected).

The National Technology Security Coalition (NTSC) is a non-profit, non-partisan organization that serves as the preeminent advocacy voice for Chief Information Security Officers (CISOs) across the United States. Through dialogue, education, and government relations, we unite both public and private sector stakeholders around policies that improve national cybersecurity standards and awareness.



4400 North Point Parkway
Suite 155
Alpharetta, GA 30022
ntsc.org

