Federal Privacy Legislation: Enforcement and State Preemption

The Insights Association supports a comprehensive federal consumer data privacy law that will respect, protect and empower consumers, and continue to allow for the informed decision-making provided by market research, insights and analytics services.

Preemption of State Laws: A Uniform National Privacy Standard

Consumers and businesses need regulatory certainty and consistency in privacy protection, and should not have to contest with a confusing, conflicting patchwork of state privacy laws (including 20 different comprehensive state privacy laws right now).

Businesses have had to invest heavily in legal and compliance consulting and extra staff just to figure out if they are covered by certain laws, let alone how to deal with such laws and ensure their practices, policies and contracts concord. Even while a relatively-similar high-level approach is followed by many states, the details vary dramatically. As a result, businesses operating across state lines must either create state-specific compliance programs or apply the most restrictive state's requirements across their entire operations. A 2022 study estimated that the state patchwork (which included a lot fewer states at the time) "could impose out-of-state costs of between $98 billion and $112 billion annually," with $20–23 billion falling specifically on small businesses.[1]

While preemption should appropriately carve out general consumer protection laws, common law torts, and certain industries, Congress should include full preemption of related state laws to avoid loopholes. For example, as happened in the 2024 American Privacy Rights Act (APRA), a broad carveout for health privacy laws from the preemption provision would have allowed the continuation of the Washington My Health My Data Act, a Washington state law presented as only about health care data, but that is written and defined so broadly that it is just another comprehensive state privacy law (albeit one with a private right of action).

Relationship to other Federal Laws

Most other federal privacy laws need to be respected. Personal information should be excluded if it is covered by and collected, processed, etc., in compliance with other federal privacy laws like GLB, FCRA, HIPAA, COPPA, TCPA, and DPPA.

Enforcement: the FTC and State AGs

The FTC has decades of experience/expertise in consumer data privacy and security issues with a designated focus on consumer protection, so the FTC should be the primary federal regulator & enforcer. Other federal agencies could assist with setting standards. State AGs (or comparable privacy enforcement authorities) could also enforce. Both the FTC and state authorities would punish violations with injunctive relief and civil penalties. Private rights of action would be prohibited. Enforcement should be delayed a year to provide covered businesses (and enforcing authorities) a chance to prepare.

[1] "The Looming Cost of a Patchwork of State Privacy Laws." ITIF. January 24, 2022. https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/