ACT | The App Association

What Innovative Small Businesses Need in a Privacy Bill

Contact Information:
tdowns@actonline.org I gdufault@actonline.org I ACTonline.org I x.com I linkedin.com

Small software and connected device companies like ACT | The App Association members handle millions of terabytes of data per day, putting them on the front lines of protecting and enabling responsible use of data. In recent years, evolving customer expectations regarding privacy have created a competitive dynamic among App Association members to meet those expectations. The App Association gives small business innovators a voice in the privacy debate in Congress and at federal agencies by illustrating how proposed laws and regulations would impact their ability to create jobs in your states and districts. However, without a federal comprehensive privacy law, businesses of every size are stuck in limbo caused by the failure of Congress to act.

In the 118th Congress, legislators put forward H.R. 8818, the American Privacy Rights Act (APRA), which sought to set a single, national set of rules for data privacy and security across all 50 states and the territories. Unfortunately, the App Association believes this bill fell short for small businesses by carving them out of both rules and protections. Small business owners want to abide by the law and be competitive in the marketplace, but they can't do that when big businesses have protections they don't.

We urge the 119th Congress to assess how any privacy legislation handles the **"4 Ps of privacy": Preemption, Protection against unauthorized access, a Path to compliance, and limits on any potential Private right of action.** If Congress strikes the right balance on these concepts, it can avoid the impending compliance tsunami from differing state laws and better enable our members to continue innovating, creating jobs, and revolutionizing industries from healthcare and education to agriculture and finance.

1 Preemption

New privacy legislation in Congress should establish a single, national set of requirements by preempting state privacy laws of general applicability that would create the most significant confusion, conflict, and compliance issues we have urged Congress to avoid.

We urge lawmakers to avoid adding so many exceptions to preemption provisions such that courts may ultimately uphold state laws that differ substantially from federal requirements. Each exception to the preemption language adds further uncertainty as to Congress' intent with respect to establishing a single set of rules rather than simply placing a federal layer on top of a divergent state patchwork.

2 Protection Against Unauthorized Access

Although most general privacy bills deal primarily with requirements surrounding consumer notice and consent for certain processing activities—along with reasonable limits on authorized processing activities—we believe they should also require covered companies to take certain steps to detect, prevent, and remediate unauthorized access to personal information. These requirements should also preempt most state laws that would otherwise impose conflicting or substantially different data security obligations. Strong federal data security provisions would raise the average readiness of American companies to defend against cyberthreats of all kinds, from state-sponsored ransomware campaigns to social engineering and phishing attacks.

3 Path to Compliance

Requirements in any privacy law should be calibrated to the underlying risk of the processing activities in question and should allow small companies to demonstrate privacy competence without being subject to immediate civil penalties for even small violations.

Going forward, privacy legislation should provide a path to ensure that smaller and less risky companies are rightfully viewed as—and held accountable for—complying with a federal framework, while alleviating liability concerns and compliance burdens that the bigger companies can more easily shoulder. One way to ensure coverage while not overburdening small businesses is a "compliance program" presumptively deeming businesses that certify adherence to industry-specific guidelines compliance to be in compliance with the law. The Children's Online Privacy Protection Act (COPPA) provides a similar compliance framework that small businesses in particular use today.

4 Private Right of Action

If a compromise federal privacy bill includes a private right of action (PRA), it must also include guardrails to prevent opportunistic litigation strategies involving a pattern of suing and settling for frivolous reasons unrelated to protecting consumers. We urge Congress to consider the needs of small businesses when determining the scope of any such right for consumers.