The SECURE Data Act Could Reduce Compliance Costs and Improve Consistency

After a decade of Congressional inaction, many states have put together a patchwork of state-level data privacy laws that apply disproportionately across the nation. This leads to competing compliance requirements and consumer rights across the states. However, the latest proposal from Congress, the SECURE Data Act (H.R. 8413), is a move in the right direction toward a uniform national standard.

Key Provisions of the SECURE Data Act

The SECURE Data Act (H.R. 8413) gives consumers familiar baseline rights: the right to access, correct, delete, and port personal data, and the right to opt out of targeted advertising, the sale of personal data, and certain profiling decisions. It also requires opt-in consent for sensitive data, creates controller and processor obligations, establishes data broker registration with the Federal Trade Commission (FTC), and relies on both FTC and state attorney general enforcement, paired with a 45-day cure period before an enforcement action may begin. The bill treats violations as violations of an FTC trade regulation rule and gives the Commission the same jurisdiction, powers, and duties it has under the FTC Act. The SECURE Data Act also expressly extends FTC enforcement to common carriers, notwithstanding the FTC Act's usual jurisdictional limits, while carving out the bill's civil-rights provision for referral to agencies with appropriate enforcement authority.

Reason Foundation Analysis

The bill is not a radical departure from where many states already stand, with the exception of California, whose privacy framework covers employee and job applicant data. It largely tracks the familiar state privacy architecture that businesses have been building toward for several years.

The most consequential provision is preemption. Section 15 says that no state or political subdivision may prescribe, maintain, or enforce a law that "relates to" the provisions of the Act. In practical terms, that means this proposal is the federal ceiling for the legislature. It is intended to displace overlapping state privacy regimes and replace the current patchwork with one national rule, harmonizing privacy rights and compliance obligations in a way that could reduce costs and improve consistency.

Similar to state bills, it establishes certain thresholds that companies need to meet to qualify. It applies to businesses that process more than 200,000 consumers' data annually and have at least $25 million in annual gross revenue, or to businesses that process at least 100,000 consumers' data and derive at least 25% of revenue from the sale of personal data. Unlike some state bills, it treats data from children and teens as

Reason Foundation Technology Policy Contact
Jen Sidorova, Policy Analyst (jen.sidorova@reason.org)

sensitive data and requires verifiable parental consent for teen data, with “teen” defined as ages 13 through 15. And unlike most state frameworks, it includes a federal data broker registration regime administered by the FTC.

The current draft does not include a data protection impact assessment requirement, even though those assessments are now standard in nearly all comprehensive state privacy laws. It also does not require businesses to honor universal opt-out mechanisms; instead, it directs the secretary of commerce to study those mechanisms and report back within three years. At the same time, the bill adds features that most state laws do not have: Commerce-approved codes of conduct; a rebuttable presumption of compliance for companies that follow approved codes; recognition of Global Cross-Border Privacy Rules certifications; and a small-business code-of-conduct pathway. Those are meaningful interoperability and compliance-design features, especially for firms trying to build scalable national businesses.

Bottom line: The SECURE Data Act deserves serious attention because it takes the familiar state privacy model and tries to solve the issues of fragmentation. The significance of the federal bill is that it would federalize a large portion of the state consensus model, making it the governing national rule. The SECURE Data Act is notably narrower on enforcement than the prior ADPPA and APRA effort, both of which included a private right of action, a provision that can lead to frivolous and burdensome litigation. It is also structurally tied to the GUARD Financial Data Act, covering the nonfinancial side while GUARD supplies the parallel federal framework for financial data.

Reason Foundation Technology Policy Contact
Jen Sidorova, Policy Analyst (jen.sidorova@reason.org)