Perspectives from FSF Scholars
September 3, 2021
Vol. 16, No. 47

Pressures Multiply for Congress to Act on Data Privacy

by

Andrew Long *

I. Introduction and Summary

It seems that each news cycle presents yet another compelling reason for Congress to pass comprehensive data privacy legislation without further delay. One day, a rival nation adopts its own law. Another day, a cyberattack with nationwide impact cries out for a unified robust federal response. Meanwhile, America's failure to act hinders efforts to reestablish a privacy shield for data transfers from the European Union, thereby causing problems for those companies engaged in transatlantic trade. And at the same time, the number of state laws imposing conflicting privacy mandates grows steadily, compounding the chaos and confusion for all involved.

Sadly, however, there is scant current evidence of meaningful legislative progress in Congress. The camel's back, it would seem, knows no limit.

Congress at last should prioritize data privacy, and legislation like the SAFE DATA Act, recently reintroduced by Senators Wicker and Blackburn, presents a promising path forward. On the key sticking points, it comes down on the right side: it would preempt state data privacy laws, whether inconsistent or not, and would not create an individual private right of action. It

also would establish what appear to be a reasonable suite of consumer privacy rights and a manageable list of compliance obligations for businesses. Just as critical, this bill would put an end to the litany of problems that arise from the current legislative vacuum at the federal level.

II. Congress's Failure to Pass Privacy Legislation Grows More Problematic by the Day

Companies and consumers alike increasingly require a single, comprehensive data privacy regime that applies nationwide. Businesses, especially small and new endeavors, would benefit from simplified, less costly compliance obligations. As I described in a March 2021 *Perspectives from FSF Scholars*, "Inconsistent State Data Privacy Laws Increase Confusion and Costs," at present companies must choose between two particularly problematic options: (1) reliance upon fallible mechanisms to associate specific customer interactions with the appropriate state, or (2) adherence to a worst-of-all-worlds compendium of the most onerous obligations established by the growing list of states that have passed data privacy legislation. Similarly, Americans clamor for one universally applicable set of easy-to-understand rights and remedies that apply without regard to where they, or the online entity with which they engage, happen to be located. In addition, both businesses and consumers would be better off if congressional action put a stop to the secondary complications that arise from the current state of affairs.

As I have written on many occasions, legislative activity at the state level presents the most compelling and obvious reason for Congress to act. Left unchecked by a preempting federal law, states increasingly are stepping in, but cyberspace is an environment for which traditional territorial boundaries have no meaning. On one side of a given transaction, highly mobile consumers may find themselves temporarily outside of their state of residence. On the other, the concept of a business's corporate headquarters has virtually no meaning or relevance. As a consequence, state-specific rules create unworkable chaos and confusion for all involved.

To date only the California Consumer Privacy Act (CCPA) has gone into effect. At present it serves as the *de facto* national data privacy regime. But well before anyone had a reasonable opportunity to become familiar with the CCPA's requirements, California voters approved the California Privacy Rights Act (CPRA), a new law that amends and expands upon the CCPA. The bulk of its provisions become operative on January 1, 2023. In the interim, businesses must adjust to the radical regulatory environment imposed by the CCPA while simultaneously preparing for the changes that the CPRA will wreak.

Meanwhile, two more states, Virginia and Colorado, have passed comprehensive data privacy laws that are similar, but not identical, to the CCPA, the CPRA, or, for that matter, each other. Once those laws are valid – the Virginia Consumer Data Protection Act at the beginning of 2023, the Colorado Privacy Act on July 1, 2023 – the situation seemingly will become untenable. Companies will face unreasonably burdensome compliance obligations, while individual consumers will require a scorecard, and possibly the assistance of legal counsel, to comprehend their rights. Further, the situation has the potential to become even worse: other states that recently have contemplated adopting their own data privacy laws include Ohio, Alaska, and Florida.

While conflicts between state laws may present the most obvious justification for increasingly vocal calls for congressional action, the lack of a federal comprehensive data privacy law creates additional, in some cases less direct, pressures. For example:

- China, of all countries, adopted a data privacy law on August 20, 2021. The Personal Information Protection Law, which goes into effect in November, is modeled on the European Union's General Data Protection Regulation ("GDPR"). Politico Morning Tech, for one, asks if "it will amp up the urgency for a federal privacy law in the U.S."

- T-Mobile discovered a data breach on August 17, 2021. The cyberattack appears to involve the information of over 50 million current, former, and prospective customers. In response, Republican leadership of the House Energy & Commerce Committee – Representatives Cathy McMorris Rodgers (R-WA), Bob Latta (R-OH), and Gus Bilirakis (R-FL) – recently asserted that "[t]his breach is yet another example of why Congress must pass a national privacy and data security law."

- From 2016 until it was invalidated by the *Schrems II* decision by the Court of Justice of the European Union in July 2020, the EU-U.S. Privacy Shield Framework facilitated transatlantic commerce by establishing "a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States." U.S. surveillance laws certainly played a prominent role in the court's reasoning, but commenters also have pointed to the lack of a U.S. federal data privacy law as a potential impediment to a successor arrangement.

  During a Senate Commerce Committee hearing in December 2020 entitled "The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows," then-Chairman Senator Roger Wicker (R-MS) posited that "I look forward to witnesses discussing how a comprehensive data privacy law with strong enforcement and meaningful privacy and redress rights for consumers might be able to aid efforts to develop a successor data transfer framework between the United States and the EU."

III. The SAFE DATA Act Offers a Potential Solution

Against this stagnant backdrop, legislation like the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act presents what appears to be a viable and productive path forward. The SAFE DATA Act was reintroduced in a revised form on July 29, 2021, by Senators Wicker, ranking member of the Senate Commerce Committee, and Marsha Blackburn (R-TN), ranking member of the Subcommittee on Consumer Protection, Product Safety, and Data Security.

I first wrote about this legislation in "Federal Privacy Legislation: Bipartisan Discussions Devolve into Dueling Drafts," a December 2019 *Perspectives*. At the time a staff discussion draft known as the United States Consumer Data Privacy Act (USCDPA), was introduced by then-Chair of the Senate Commerce Committee Wicker after the failure of what at one point appeared to be promising negotiations involving lawmakers from both political parties. As I noted in a

contemporaneous blog post, the USCDPA was introduced for the first time as the SAFE DATA Act on September 17, 2020.

In its current form, the SAFE DATA Act would apply to non-profits and common carriers in addition to other businesses generally subject to the FTC's jurisdiction under the FTC Act. Certain small businesses would be exempt. It would cover personal information that "identifies or is linked or reasonably linkable to an individual or a device that is linked or reasonably linkable to an individual." In addition, it would:

- Empower consumers with rights to know, access, correct, delete, and port their data – and protect them from discriminatory treatment for exercising those rights.
- Require opt-in consent only for "sensitive covered data," which it defines to include government-issued identifiers, such as a Social Security or driver's license number; health data; financial and account log-in credentials; biometric and GPS information; racial, ethnic, or religious identity; sexual orientation; and private communications, including emails and texts.
- Allow consumers to opt out of the use of non-sensitive personal information.
- Direct businesses to make privacy policies available in a clear and conspicuous manner, use personal data only to the extent that is "reasonably necessary" and consistent with said privacy policies, perform regular privacy impact assessments, and maintain reasonable data security programs.
- Expressly prohibit companies "from processing data in ways that violate federal Civil rights laws."
- Appropriate to the FTC $100 million to bolster its ability to carry out its expanded privacy enforcement responsibilities.
- Provide the FTC with limited rulemaking power.
- Preempt broadly any state or local laws "related to the data privacy or data security and associated activities of covered entities."

The SAFE DATA Act would *not* provide for an individual private right of action. The FTC would be empowered to enforce it in the same way that it enforces the FTC Act. In addition, state attorneys general could bring civil actions in federal court.

Should the SAFE DATA Act be signed into law, it would go into effect 18 months thereafter.

IV. Conclusion

As we unfortunately have witnessed over the last several years, accumulating facts on the ground, no matter how dire, have not been able to establish the momentum necessary to break through the logjam that persists on the Hill. It therefore would be foolish to suggest that the spotlight cast by the most recent privacy-related developments – China passing its own comprehensive data privacy law, the T-Mobile cyberattack, a lack of progress on reestablishing a data privacy shield with the European Union, the third state adopting its own unique legislation – might, at last, prompt Congress to adopt comprehensive data privacy legislation.

Should lawmakers endeavor to conquer this difficult issue, however, legislation like the SAFE DATA Act presents a promising solution. Among other things, it would create what appear to be reasonable consumer privacy rights and related corporate responsibilities, preempt the expanding list of problematic state data privacy laws, reject an individual private right of action, and authorize, as well as adequately fund, effective enforcement by the FTC.

* Andrew Long is a Senior Fellow of the Free State Foundation, an independent**,** nonpartisan free market-oriented think tank located in Rockville, Maryland. The views expressed in this *Perspectives* do not necessarily reflect the views of others on the staff of the Free State Foundation or those affiliated with it.

Further Readings

"Ohio Legislators Introduce the Latest Comprehensive State Data Privacy Bill," *FSF Blog* (July 20, 2021).

"Exhibit C(O) in the Case for a Federal Data Privacy Law: The Colorado Privacy Act," *FSF Blog* (July 15, 2021).

"Alaska Is the Latest State to Propose a Data Privacy Law," *FSF Blog* (April 9, 2021).

"Colorado Lawmakers Introduce Data Privacy Bill," *FSF Blog* (April 6, 2021).

"Inconsistent State Data Privacy Laws Increase Confusion and Costs," *Perspectives from FSF Scholars*, Vol. 16, No. 14 (March 16, 2021).

"Florida Vies for Bronze in Race to Create Patchwork of State Data Privacy Laws," *FSF Blog* (March 12, 2021).

"Virginia's Consumer Data Protection Act Soon Could Become Law," *FSF Blog* (February 5, 2021).

"California Voters Approve the California Privacy Rights Act: A Detailed Analysis of Its Requirements and Impact," *Perspectives from FSF Scholars*, Vol. 15, No. 60 (November 17, 2020).

"Privacy Recap: Senate Commerce Committee Holds Hearing, Republican Members Introduce SAFE DATA Act," *FSF Blog* (September 25, 2020).

"California Privacy Regulation Must Account for the COVID-19 Crisis," *Perspectives from FSF Scholars*, Vol. 15, No. 26 (May 27, 2020).

"A Privacy Private Right of Action Is Inferior to FTC Enforcement," *Perspectives from FSF Scholars*, Vol. 15, No. 4 (January 21, 2020).

"Federal Privacy Legislation: Bipartisan Discussions Devolve into Dueling Drafts," *Perspectives from FSF Scholars*, Vol. 14, No. 42 (December 4, 2019).

"California's Privacy Law: Recent Developments Underscore the Need for Preemptive Federal Law," *FSF Blog* (November 21, 2019).

"California's Heavy-Handed Approach to Protecting Consumer Privacy: Exhibit A in the Case for Federal Preemption," *Perspectives from FSF Scholars*, Vol. 14, No. 35 (October 28, 2019).