Perspectives from FSF Scholars
January 6, 2022
Vol. 17, No. 2

A Tale of Three Data Privacy Bills: Federal Legislative Stalemate Enables Bad State Laws

by

Andrew Long *

I. Introduction and Summary

It has been self-evident for years that consumers and businesses alike would be best served by a single set of federal data privacy rules that, like the Internet itself, knows no state boundaries. And yet the wait for Congress to act continues. Three recently introduced pieces of legislation, two at the federal level and one in Massachusetts, demonstrate the two primary reasons that a nationwide data privacy regime does not yet exist – as well as why it is so important that one quickly comes into being.

In the House of Representatives, recent rival bills remind us of the biggest sticking points: (1) whether it is necessary for a comprehensive federal data law to preempt the growing list of inconsistent state laws (it is), and (2) whether a private right of action is an appropriate enforcement mechanism to protect individual rights (it is not). The third legislative proposal is yet another insular state-specific approach, one that, by going even further than the laws already

passed in California, Virginia, and Colorado, proves conclusively that a preemptive federal law that rejects a private right of action is the only sensible path forward.

Over the years, of course, numerous comprehensive data privacy bills have been introduced in both the House and the Senate. The extensive "Further Readings" section at the end of this *Perspectives* includes papers that contain detailed summaries of several such proposals. To a large degree, they all hew to a similar framework: (1) define the specific types of personal information and/or "sensitive" personal information that is covered; (2) enumerate a list of rights, such as the right to know, request, delete and/or correct data that is collected; (3) provide consumers with a say as to whether and when their personal information is shared or sold; (4) define which businesses are covered; (5) require covered businesses to notify customers about their data collection practices; and so on.

On the margins, however, they tend to differ in significant respects. By way of example, some propose that an entirely new agency be created, while others recognize, and in many cases expand, the longstanding and time-tested role played by the FTC. Some require consumers to opt-in to the use of any of their personal information, while others embrace a more reasonable and realistic opt-out model for non-sensitive data.

Most importantly, however, these various legislative proposals take diametrically opposed positions on two highly contentious – and, to date, insurmountable – issues. The first is whether federal legislation should supersede conflicting and/or more expansive state laws. As I argued most recently in "Inconsistent State Data Privacy Laws Increase Confusion and Costs," a March 2021 *Perspectives from FSF Scholars*, the expanding list of states that have adopted their own unique comprehensive data privacy laws – currently at three: California (twice), Virginia, and Colorado – creates confusion for consumers and unreasonably burdensome compliance headaches for companies, in particular small businesses and start-ups, that operate across the entire online space, not solely within specific state boundaries. Accordingly, one of the most critical functions that a comprehensive federal data privacy law should perform is to establish a single regime that applies nationwide – and do so by expressly preempting any and all related state laws.

The second is whether individuals should be authorized to pursue civil remedies for alleged violations. There is no question that the measure of a comprehensive federal data privacy law's efficacy is whether it includes one or more meaningful enforcement mechanisms. The approach that I advocated in "A Privacy Private Right of Action Is Inferior to FTC Enforcement," a January 2020 *Perspectives*, relies upon continued case-by-case oversight by the FTC, the agency with substantial institutional subject-matter knowledge and experience in this area, bolstered by expanded authority (for example, the ability to impose fines for first-time offenses and limited privacy rulemaking abilities) along with additional resources (that is, an expanded budget that allows additional hires). By contrast, a private right of action creates inappropriate incentives to file unwarranted class-action lawsuits and is more likely to benefit the plaintiffs' bar than aggrieved individuals.

Unfortunately, not everyone shares my views on these issues. Some lawmakers do, of course. Others embrace the contrary view. However, there is one thing upon which they all do seem to

agree: whatever their particular position, it stands as a dealbreaker. Consequently, despite repeated attempts to achieve a middle ground, a workable compromise remains out of reach. Two bills introduced in the House during November 2021 stand as the most recent examples of this persistent divide.

II. Partisan Legislative Proposals Expose the Two Hurdles to Federal Progress

On November 3, 2021, Republicans on the House Energy and Commerce Committee, led by Representative Cathy McMorris Rodgers (WA), announced a multiprong effort to advance a national privacy standard. Central to that strategy is a discussion draft, the Control Our Data Act, that incorporates four principles: an approach that "does not stop at state lines"; that ensures consumers "understand how their information is collected, used, and shared"; that demands businesses adopt "reasonable measures to protect people's personal information"; and that does not unnecessarily impede innovation – "[w]e want small businesses hiring coders and engineers, not lawyers."

The Control Our Data Act would preempt state laws. Section 112(a)(1) states broadly that:

> No State or political subdivision of a State may maintain, enforce, prescribe, or continue in effect any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State, or political subdivision of a State, related to the collection, use, or sharing of personal information by or on behalf of a covered entity.

Pursuant to Section 113(f), "[n]othing in this Title shall be construed to establish a private right of action." Instead, violations of the Control Our Data Act would "be treated as an unfair and deceptive act or practice in violation … of the Federal Trade Commission Act." Businesses would be afforded a 30-day right to cure alleged violations. The FTC would be responsible for enforcement, which would encompass civil penalties, including for first-time offenses. State attorneys general (and other consumer protection officers otherwise authorized by the states) also would be empowered to bring civil actions, subject to intervention by the FTC.

At the opposite end of the spectrum is the Online Privacy Act, reintroduced by California Democrats Anna G. Eshoo and Zoe Lofgren on November 18, 2021. I first addressed the Online Privacy Act in a post to the *FSF Blog* shortly after it was unveiled in November 2019. Because the Online Privacy Act is silent on the issue of preemption, it appears to invite a nightmare scenario where, even with a federal law in place, the specific rules, rights, and responsibilities that apply would continue to vary from state to state.

The Online Privacy Act similarly comes down on the wrong side with respect to a private right of action. Section 405 would authorize a "person who is aggrieved by a violation of this Act" to pursue declaratory or injunctive relief as well as a civil action for damages on an individual basis. Moreover, where represented by a designated non-profit organization, they could do so on a collective (that is, class action) basis.

III. Legislation Proposed in Massachusetts Underscores the Need to Preempt State Laws

Were it the case that the failure of federal lawmakers to resolve their disagreements on preemption and enforcement resulted only in further delay and general uncertainty, continued oversight by the FTC might serve as an adequate stop gap. But instead, the absence of a preemptive federal law has opened the door to state laws – two in California, one in Virginia, and one in Colorado. The similar, but by no means identical, approaches embodied therein are a recipe for chaos – and thus prove the case for preemption. Of even greater concern, a bill recently introduced in Massachusetts serves as definitive proof why a private right of action is an unworkable idea.

First filed in February 2021, the Massachusetts Information Privacy Act in its current draft form embraces a position on private rights of action more extreme than any other state to date. Subsection 14(a) states expansively that "[a]ny individual alleging a violation of this chapter or a regulation promulgated under this chapter may bring a civil action in any court of competent jurisdiction." Subsection 14(a)(1) makes clear that an individual need not file an administrative complaint before initiating a civil action for damages.

Most alarmingly, subsection 14(a)(4) allows for "liquidated damages *of not less than* 0.15% of the annual global revenue of the covered entity or $15,000 per violation, *whichever is greater*" (emphasis added), as well as punitive damages. And subsection 14(a)(5) authorizes the award of "reasonable attorney's fees and costs to any prevailing plaintiff." As one commenter noted, should this proposal become law, it would "make Massachusetts the go-to jurisdiction for the class action plaintiffs bar."

IV. Conclusion

Thus far, congressional inaction on data privacy certainly has raised alarms. And it has denied both consumers and companies the benefits associated with a single set of proper national rules. But it hasn't yet led to outright chaos. Of the four state laws passed to date, only one, the California Consumer Privacy Act (CCPA), actually has gone into effect. As a result, and because of California's huge population, currently that law serves as the *de facto* national privacy regulation. This is a problem, to be sure – Congress, not the California legislature, should determine federal data privacy policy – but at least only one set of rights and responsibilities apply. Soon, however, that will change. The Virginia Consumer Data Protection Act becomes law on January 1, 2023, the same day as the California Privacy Rights Act, which modifies the CCPA. The Colorado Privacy Act becomes effective six months later. Absent a preemptive federal law, the dreaded "patchwork" of inconsistent state laws will be upon us in less than a year's time. And as the Massachusetts Information Privacy Act foretells, future state laws hold the potential to make the situation far worse.

However, there may be at least a small sliver of hope: according to *Politico*, Chair Janice D. Schakowsky (D-IL) announced at a December 9, 2021, Consumer Protection & Commerce subcommittee hearing on Big Tech accountability that Democrats on the full House Energy & Commerce Committee had shared a draft data privacy bill with their Republican colleagues the week prior – and that she intends to hold a hearing on the subject early this year. Should that

come to pass, it would be the first of its kind convened during the 117th Congress, and – never say never – might ultimately produce an acceptable compromise on data privacy. Specifically, one that results in a preemptive federal law that rejects a private right of action.

* 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

"Privacy Recap: Senate Commerce Committee Holds Hearing on Data Privacy; Op-Ed Authors Oppose FTC Privacy Rulemaking," *FSF Blog* (October 1, 2021).

"FTC Commissioner Wilson Recruits Student Researchers to Inform and Inspire Efforts to Pass a Federal Data Privacy Law," *FSF Blog* (September 29, 2021).

"Congressional Testimony of FTC Commissioner Wilson Addresses Agency Processes, Section 13(b), and Federal Privacy Legislation," *FSF Blog* (July 29, 2021).

"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).

"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).