Perspectives from FSF Scholars
February 3, 2023
Vol. 18, No. 6

In 2023, the Congressional Privacy Impasse Could Reach Its Breaking Point

by

Andrew Long *

I. Introduction and Summary

The early days of 2023 present an opportunity to reflect upon the data privacy regulatory and legislative status quo. In short, congressional inaction fosters an increasingly untenable situation for both consumers and companies. Once-theoretical concerns about a "patchwork" of rival state regimes are now a practical reality. The Federal Trade Commission's ill-conceived "digital surveillance" rulemaking – which could layer *additional* regulations on top of the multistate morass – has been joined by a problematic National Telecommunications & Information Administration proceeding. All the while, commentators prognosticate on the prospects that this session Congress finally might pass a federal comprehensive data privacy law – invoking renewed optimism or an unsettling sense of déjà vu, depending on your disposition.

While it remains to be seen whether Congress in fact *will* act, there is no question that our elected federal representatives – not the states, and not the Biden administration acting unilaterally – *should* establish clear and consistent nationwide privacy rules of the road. And, for the following reasons, do so without delay:

The Free State Foundation
P.O. Box 60680, Potomac, MD 20859
info@freestatefoundation.org
www.freestatefoundation.org

- On January 1, California's first-ever state comprehensive data privacy law, just two years old, was amended, and expanded, by Proposition 24. Confusingly, however, those changes are not enforceable until July 1. Which arguably is a good thing, as the state privacy agency responsible for promulgating and implementing rules failed to do so in a timely manner.
- Also on January 1, the Virginia Consumer Data Protection Act went into effect – and in doing so, rendered real the dreaded "patchwork" of multiple, inconsistent state laws.
- Three more already-enacted state laws – in Colorado, Connecticut, and Utah – will further complicate the landscape later this year as they become effective.
- As many as 14 additional state legislatures currently are considering their own data privacy laws – threatening to create an impossibly confusing situation for consumers and a compliance nightmare for businesses, in particular small operations.
- The Federal Trade Commission's active and unbounded "digital surveillance" rulemaking promises to impose yet another layer of costly regulations on top of those imposed by the states. And the National Telecommunications and Information Administration, seemingly prompted by a recent op-ed by President Biden, also has jumped into the fray.

These developments, both realized and looming, exacerbate an already untenable situation. By contrast, what consumers deserve is a single set of simple-to-understand privacy rights that apply across the borderless Internet. And what companies require are workable obligations designed to realize those consumer rights without imposing unreasonable costs or unduly impeding popular advertising-supported ("free") services.

Only Congress, through the negotiation and passage of a comprehensive data privacy law, which expressly preempts state laws that impose requirements beyond those contained in, or inconsistent with, the federal law, can accomplish those critical goals. There should be bipartisan support for enacting such legislation.

II. The Privacy Status Quo Compels a Preemptive Congressional Response

To fully grasp the severity of the situation, it is helpful to consider where congressional inaction has led us.

At the beginning of 2020, the California Consumer Privacy Act (CCPA), the nation's first state-specific comprehensive data privacy statute, became law – and assumed the role of *de facto* national privacy approach. Given California's size and prominence in the digital economy, along with the inherent risk that efforts to associate virtual customer-company interactions with specific physical locations may fail, many businesses made the rational decision to comply with the CCPA nationwide. The CCPA tasked the Office of the California Attorney General with rulemaking responsibilities – a job that, after much uncertainty producing drama, it belatedly completed – and enforcement authority. The latter, most notably, led to a $1.2 million settlement with Sephora, Inc., in August 2022.

On July 20, 2022, a federal privacy bill – the American Data Privacy and Protection Act (ADPPA) – for the first time made it out of committee: on a 53-2 vote, the House Committee on

Energy and Commerce approved an amended version of the ADPPA. Sadly, it did not make it to the House floor during the last Congress.

On August 11, 2022, the Federal Trade Commission (FTC) announced the adoption of an Advance Notice of Proposed Rulemaking on "commercial surveillance and data security." As the Free State Foundation pointed out in responsive comments, this misguided effort, among other things, would do nothing to solve the "patchwork" problem of multiple, inconsistent state approaches – to the contrary, it would add an additional federal layer to, rather than preempt, state laws.

On January 1, 2023, the California Privacy Rights Act (CPRA) became effective – but not yet enforceable – law. (The first-of-its-kind California Privacy Protection Agency (CPPA), which was created by the CPRA, cannot begin to enforce the CPRA until July 1.) As I detailed in a November 2020 *Perspectives from FSF Scholars*, the CPRA modifies and expands upon the CCPA in a number of ways. In addition, it transfers to the CPPA the Office of the Attorney General's rulemaking responsibilities. Unfortunately, the CPPA has followed in its predecessor's footsteps, failing to finalize regulations on time.

That same day, the Virginia Consumer Data Protection Act made real the long-held theoretical concern regarding multiple, overlapping, and contradictory state statutes that I described in the March 2021 *Perspectives*, "Inconsistent State Data Privacy Laws Increase Confusion and Costs.

In a *Wall Street Journal* op-ed published on January 11, 2023, President Biden called for Congress "to pass strong bipartisan legislation to hold Big Tech accountable" that imposes "clear limits on how companies can collect, use and share highly personal data." More specifically, he argued in favor of:

> [S]erious federal protections for Americans' privacy. That means clear limits on how companies can collect, use and share highly personal data – your internet history, your personal communications, your location, and your health, genetic and biometric data. It's not enough for companies to disclose what data they're collecting. Much of that data shouldn't be collected in the first place. These protections should be even stronger for young people, who are especially vulnerable online. We should limit targeted advertising and ban it altogether for children.

In response, House Energy and Commerce Chair Cathy McMorris Rodgers (R-WA) stated that, "[r]ather than trying to address these harms unilaterally through executive action and contorting authority, the administration needs to work with Congress to enact comprehensive privacy protections through one national privacy standard that protects all Americans, especially our kids."

On that note, in a press release dated January 18, 2023, the National Telecommunications and Information Administration (NTIA) announced that it was launching an inquiry regarding "how companies' data practices may impose outsized harm on marginalized or underserved communities." A Privacy, Equity, and Civil Rights Request for Comment was published in the

Federal Register two days later. As is the case with the "digital surveillance" rulemaking underway at the FTC, any rules promulgated by NTIA would, among other things, (1) add to, rather than preempt, existing state laws, and (2) likely run afoul of the Supreme Court's invocation of the "major questions doctrine" in 2022's *West Virginia v. EPA*.

Looking ahead, 2023 promises additional complications. On July 1, 2023, two more state-specific laws – the Colorado Privacy Act and Connecticut's "An Act Concerning Personal Data Privacy and Online Monitoring" – will further muddle the regulatory landscape for both consumers and companies. And on New Year's Eve 2023, the Utah Consumer Privacy Act will join the privacy "patchwork" party.

According to the International Association of Privacy Professionals (IAPP), as of January 27, 2023, 14 state legislatures are considering their own comprehensive data privacy bills. "The Looming Cost of a Patchwork of State Privacy Laws," a January 2022 report published by the Information Technology & Innovation Foundation, concluded that "[s]tate privacy laws could impose out-of-state costs of between $98 billion and $112 billion annually. Over a 10-year period, these out-of-state costs would exceed $1 trillion." Small businesses – that is, those least able to absorb such unnecessary and wasteful expenses – would be on the hook for as much as one-fifth of that total.

III. Conclusion

As I explained in March 2021's "Inconsistent State Data Privacy Laws Increase Confusion and Costs," balkanized responses to a border-defying concern like data privacy create more problems than they solve. Consumers, already struggling to stay informed in an online environment evolving at the speed of light, must try to discern for themselves what rights they have based upon unclear geographic divisions. Companies, meanwhile, must choose between two unpleasant paths: one, establish multiple compliance programs along with a robust mechanism to associate each customer with the appropriate state; or two, adhere to an evolving worst-of-all-worlds litany of the most onerous aspects of each state law.

With the dawning of 2023, Virginia has become the second state with an effective and enforceable privacy law. Consequently, what were once theoretical concerns regarding contradictory state-level data privacy regimes are now headache-causing inefficiencies enabled by the inability of Congress to finalize comprehensive federal data privacy legislation which expressly preempts state laws that impose requirements beyond those contained in, or inconsistent with, the federal law. And given that three more state statutes will become law in the next twelve months, additional states likely will pass their own unique laws, and multiple federal agencies appear poised to further muddy the waters, the already intense pressure for Congress to act surely and steadily will increase.

* 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

Comments of the Free State Foundation, *Commercial Surveillance ANPR, R111004* (November 16, 2022).

Andrew Long, "Privacy Recap: Regulatory Developments in California, Colorado," *FSF Blog* (October 25, 2022).

Andrew Long, "Expanding Cracks Threaten the Privacy Preemption Legislative Compromise," *Perspectives from FSF Scholars*, Vol. 17, No. 48 (September 23, 2022).

Andrew Long, "FTC Initiates Privacy Rulemaking Despite Congressional Momentum: Republican Commissioners Issue Strong Dissents," *FSF Blog* (August 18, 2022).

Andrew Long, "House Commerce Committee Passes Amended Privacy Bill, Concerns Remain," *Perspectives from FSF Scholars*, Vol. 17, No. 39 (August 4, 2022).

Andrew Long, "Bipartisan Privacy Discussion Draft: Significant, If Incomplete, Progress," *Perspectives from FSF Scholars*, Vol. 17, No. 32 (June 16, 2022).

Andrew Long, "#FSFConf14 Speakers on Need for Federal Privacy Law," *FSF Blog* (May 26, 2022).

Andrew Long, "Utah Becomes Fourth State to Pass a Privacy Law," *FSF Blog* ((March 25, 2022).

Andrew Long, "A Tale of Three Data Privacy Bills: Federal Legislative Stalemate Enables Bad State Laws," *Perspectives from FSF Scholars*, Vol. 17, No. 2 (January 6, 2022).

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

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

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

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

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

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

Andrew Long, "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).

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

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

Andrew Long, "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).