Perspectives from FSF Scholars
July 24, 2023
Vol. 18, No. 31

More States Compound the Dreaded Privacy "Patchwork" Problem

by

Andrew Long *

I. Introduction and Summary

The dizzying pace of state-level data privacy activity makes it hard to keep up. What's more, the resulting "patchwork" of laws has become so complicated that interested observers can no longer agree even on the precise number of comprehensive data privacy statutes that have been passed. That fact alone speaks volumes about how difficult it has become for both companies and consumers to make sense of the ever-evolving regulatory landscape – and how important it is for Congress to establish a uniform national data privacy framework that preempts state laws.

And a federal floor upon which states might build would be little better than the current situation.

What is clear: on July 1, the number of states with in-effect privacy laws doubled from two to four, with one more poised to join that group at the end of this year. At least six additional state laws have been passed. And one more awaits the governor's signature.

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

At the federal level, meanwhile, there has been little progress of note since the American Data Privacy and Protection Act cleared the House Commerce Committee last July. Unless Congress acts, there is an increasing risk that the "patchwork" of state laws, containing often conflicting varying requirements, may well result in so much consumer confusion that there will be less online engagement. This decreased consumer engagement will result in overall consumer welfare losses.

Similarly, the increased costs attributable to the resources required to set up and maintain operational systems that track and implement ongoing changes in the various state privacy laws is substantial and could lead to a diminishment in the quantity and quality of applications. This is separate and apart from the costs imposed by any state law information collection, disclosure, and retention requirements or liability provisions where the overall costs exceed the benefits.

II. A Scorecard Is Needed to Follow the State-Level Action

State-level data privacy regulation formally commenced on January 1, 2020, when the California Consumer Privacy Act (CCPA) became enforceable law. That statute was modified by the California Privacy Rights Act (CPRA), which went into effect on January 1 of this year. (Though too convoluted to detail here, both the CCPA and the CPRA required regulators – in the case of the CCPA, the State Attorney General's office, and for the CPRA, the first-of-its-kind California Privacy Protection Agency established by the CPRA – to promulgate implementing rules. In both instances, those proceedings experienced delays. In fact, the effective date for some of the rules implementing the CPRA recently was pushed back to March 2024 by the Sacramento County Superior Court as a consequence of a missed statutory deadline.)

New Year's Day 2023 then made real the long-feared compliance challenge of overlapping/inconsistent state laws: as I described in a February 2023 *Perspectives from FSF Scholars*, the Virginia Consumer Data Protection Act on that day became the second enforceable comprehensive data privacy statute.

And on July 1, both the Colorado Privacy Act (as well as its implementing rules) and Connecticut's "An Act Concerning Personal Data Privacy and Online Monitoring" went into effect, bringing the total to four. (The Utah Consumer Privacy Act will up that number to five at the end of 2023.) To make matters even more confusing, Connecticut's law was amended by legislation passed less than a month earlier – and those revisions have staggered start dates of October 1, 2023 (provisions concerning consumer health data), January 1, 2024 (dating app operators), July 1, 2024 (social media platforms), and October 1, 2024 (businesses whose offerings are used by those under the age of 18).

Thus, already the situation is untenable. As I pointed out more than two years ago in "Inconsistent State Data Privacy Laws Increase Confusion and Costs," a *Perspectives from FSF Scholars* paper, neither consumers nor companies are served when the applicability criteria, specific list of enumerated consumer rights, and corporate responsibilities vary from state to state.

And with each new state action, potentially covered businesses and their outside attorneys (assuming a business can afford them, which is not always the case, particularly with respect to smaller firms and innovative new start-ups) once again must parse dense language to determine whether they are covered and, if so, what nuanced obligations they must abide. As highlighted above, sometimes that analysis must consider multiple statutes, as is the case in California and Connecticut, as well as implementing rules. Meanwhile, it seems highly unlikely that consumers are able to appreciate what rights they have, and from which states those rights emanate.

Seemingly with each passing day, however, the regulatory environment becomes ever more complicated. With little progress of note on Capitol Hill (beyond the looming promise of the long-stalled American Data Privacy and Protection Act and a few hearings held this session), more and more states are taking action.

In contemporaneous blog posts, I have highlighted statutes passed in Iowa (state number six), Indiana (state number seven), Tennessee (state number eight), and Montana (state number nine). Though in many ways similar, each of these laws includes provisions that separate them from the pack. Some examples:

- Unlike many other state statutes, Iowa Senate File (SF) 262, "an Act relating to consumer data protection, providing civil penalties, and including effective date provisions," eschews a revenue threshold, instead focusing exclusively on the number of state residents for whom a business controls or processes personal data.
- Recognizing that much can be learned from observing how other states fare, the Indiana Consumer Data Privacy Act establishes a relatively late effective date: July 1, 2026.
- The Tennessee Information Protection Act requires covered businesses to conform their privacy compliance programs to the National Institute of Standards and Technology privacy framework.
- The Montana Consumer Data Privacy Act, in an apparent nod to that state's relatively low population, applies to businesses that process the personal information of only 50,000 residents. (Most other states set that bar at 100,000.)

In the interim, still more states have adopted comprehensive data privacy statutes. Exactly how many, however, is a matter up for debate. The privacy "patchwork" isn't just growing. It's also evolving in terms of topics addressed in a way that no Venn diagram can comprehensibly capture.

Interested observers generally agree that the following bills all fit the description:

- The Texas Data Privacy and Security Act (TDPSA), signed into law on June 18, 2023. The TDPSA forges its own path with respect to determining which businesses are covered. Rather than determine applicability based on a revenue or number-of-residents threshold, it casts a wider net: any entity that operates in the state, processes or sells personal data, and does not fall with the definition of a "small business"

(which, it turns out, is an unexpectedly convoluted, industry-specific matter to determine) is on the hook.

- The Oregon Consumer Privacy Act (OCPA), which the governor signed on July 18, 2023. Unlike any other comprehensive data privacy law, the OCPA empowers consumers to request the *specific list* of third parties to whom a covered business has disclosed personal data. (Other states require that covered businesses provide only a list of the *categories* of third parties with which personal data is shared.)
- The Delaware Personal Data Privacy Act (DPDPA), which cleared the legislature on June 30, 2023. Similar to the Montana Consumer Data Privacy Act, the DPDPA sets a relatively low bar in terms of affected residents in response to the state's small size: 35,000 (as compared to 50,000 in Montana and 100,000 in most other states).

And then there is the Florida Digital Bill of Rights (FDBR). Signed into law on June 6, 2023, the FDBR (1) sets the annual gross revenue bar for a covered "controller" exceedingly high: $1 billion, and (2) incorporates other requirements (relating to online advertising, smart speakers, and app stores) that limit applicability to a fairly small universe of businesses. As such, some observers do not consider the FDBR to be a *comprehensive* data privacy law.

However, the FDBR's provisions regarding "sensitive personal data" apply to all for-profit businesses – not just those that meet the definition of a "controller" referenced above. Accordingly, Keir Lamont, Director at the Future of Privacy Forum, wrote in the June 9, 2023, edition of The Patchwork Dispatch newsletter that "[g]iven that the bulk of SB 262's privacy requirements will only directly apply to small set of very large companies in specific lines of business, the Dispatch's editorial team has decided not to treat it as a 'comprehensive' privacy law."

From a regulatory perspective, though, this distinction misses the point. The growing privacy "patchwork" burdens businesses, particularly small businesses, in several ways. One, of course, is through the imposition of new compliance obligations that vary, to a greater or lesser extent, from state to state. But another relates to the increasingly byzantine and costly analyses that companies and their legal counsel must engage in at the outset – and in response to subsequent legislative and/or regulatory developments – to determine if, and to what extent, the law even applies to them. Because certain provisions of the FDBR do apply to all for-profit businesses that operate in Florida and process sensitive personal data, it undeniably represents yet another item on the growing list of data privacy statutes with which businesses must grapple.

III. Conclusion

Having incorrectly identified, on more than one occasion, what I believed to be the proverbial "straw that breaks the camel's back," I will refrain from once again suggesting that the latest wave of state-specific data privacy activity might inspire Congress, at long last, to act. However, I will repeat the following two undeniable and urgent truths.

The first is that consumers deserve a single, consistent set of privacy rights that are easy to understand and apply nationwide, and the only way to realize that goal is through the passage

of a federal comprehensive data privacy law that preempts – to be clear, I mean fully preempts; a mere floor upon which states are allowed to build would do nothing to clear up the confusion – the growing list of state-level statutes that make up the dreaded privacy "patchwork."

The second truth is that the increasingly complicated regulatory landscape that companies face imposes unjustified compliance costs that create inefficiencies and particularly burdens small businesses.

* 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

Andrew Long, "Montana Makes Nine: Another State Passes a Data Privacy Law," *FSF Blog* (June 6, 2023).

Andrew Long, "Tennessee Is State Number Eight to Pass a Privacy Law," *FSF Blog* (May 18, 2023).

Andrew Long, "Seven States and Counting: Indiana Passes Privacy Law," *FSF Blog* (May 5, 2023).

Andrew Long, "Iowa Is State No. 6 to Pass a Privacy Statute," *FSF Blog* (March 31, 2023).

Andrew Long, "In 2023, the Congressional Privacy Impasse Could Reach Its Breaking Point," *Perspectives from FSF Scholars*, Vol. 18, No. 6 (February 3, 2023).

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