Perspectives from FSF Scholars
May 9, 2025
Vol. 20, No. 21

A Congressional Working Group Takes a Fresh Look at Data Privacy: Now Congress Should Act

by

Andrew Long *

I. Introduction and Summary

In April, the California Privacy Protection Agency and seven state Attorneys General upped the privacy "patchwork" ante with the creation of the Consortium of Privacy Regulators. As if 20 (and counting) inconsistent state-specific comprehensive data privacy statutes weren't sufficiently concerning, especially for small businesses and start-ups for whom compliance costs are a significant concern, now there is a multistate coalition whose stated mission is to "coordinate efforts to investigate potential violations of applicable laws" and "coordinate[] enforcement." This might result in a "patchwork" within a "patchwork." After all, the parties themselves readily concede that "each state has its own law."

Fortunately, and as I described in contemporaneous posts to the *FSF Blog*, Republican lawmakers on the House Commerce Committee have created a working group and solicited public input regarding the specific provisions a federal privacy bill ought to include. As I have written on countless occasions, most recently in a December 2024 *Perspectives from FSF Scholars*, a new federal data privacy law must (1) strike the appropriate balance between

safeguarding consumer's personal information and fostering consumer-benefiting innovation; (2) preempt inconsistent state laws, especially in connection with Artificial Intelligence (AI); (3) end the disparate and often duplicative oversight by the Federal Communications Commission of communications providers vis-à-vis similarly situated competitors in the online ecosystem; (4) reject a private right of action; and (5) entrust the Federal Trade Commission with exclusive enforcement powers.

Now, it's time for lawmakers to reach agreement on statutory language that embodies these key points so that consumers' legitimate privacy expectations will be met, while, at the same time, online providers will retain the freedom to continue to invest and innovate without being inhibited by unnecessary or unduly burdensome regulation and mandates.

II. Republican House Commerce Committee Members Reboot Federal Legislative Privacy Efforts by Creating Working Group, Soliciting Public Input

In February, House Commerce Committee Chairman Brett Guthrie (R-KY) and Vice Chairman John Joyce, M.D. (R-PA) created a data privacy working group comprised of Republican committee members in order "to bring members and stakeholders together to explore a framework for legislation that can get across the finish line." In the last few years there have been two noteworthy, but ultimately unsuccessful, attempts to pilot a comprehensive data privacy bill through Congress: 2024's American Privacy Rights Act (APRA), the abrupt demise of which I detailed in a December *Perspectives from FSF Scholars*, and 2022's American Data Privacy and Protection Act (ADPPA), the focus of "Expanding Cracks Threaten the Privacy Preemption Legislative Compromise," a September 2022 *Perspectives*. In both instances, fundamental disagreements regarding the preemption of state laws and a private right of action brought forward momentum to a halt.

So as not to repeat the mistakes of the past, the working group embraced a novel approach – specifically, rather than drafting a bill first and soliciting feedback second, it wiped the slate clean and, as its first order of business, issued a Request for Information (RFI) on February 21, 2025. The RFI sought input from the public on a wide range of issues, including:

- What types of entities interact with personal information and what specific obligations should apply;
- What specific consumer rights (the right to know, the right to correct, the right to delete, and so on) federal privacy legislation should codify regarding both personal information and sensitive personal information and how those rights should be communicated to the public;
- What lessons can be gleaned from state-level privacy activities and to what extent state privacy laws should be preempted;
- What steps entities should be required to take to ensure the security of consumer data;
- What role, if any, individual states should play in the oversight of AI; and

- What the pros and cons are of exclusive enforcement by the FTC and state Attorneys General and whether a federal privacy regime should include a safe harbor.

On this last point, the RFI notably avoided specific mention of a private right of action.

According to *Law360* (subscription required), over 250 interested parties submitted comments. And while the working group to date has not made those filings available on the committee's website, some commenters have posted their submission on their own websites or made them available to press outlets such as *VitalLaw* (subscription required). The discussion below references a number of those comments and, where possible, provides public-facing links.

III. Consumers and Businesses Alike Deserve Clear and Consistent Rules of the Road

The RFI solicits detailed responses on the appropriate responsibilities of businesses, rights of consumers, and roles of individual states. Zooming out, however, it is important and helpful to acknowledge the basic principles that should inform a federal data privacy regime.

Consumers deserve to understand with relative ease what rights and recourses they have regarding the use, and potential misuse, of their personal information. A criticism directed at the notice-and-consent framework is that privacy notices not surprisingly tend to be highly technical and heavy on the details. A uniform set of definitions – in particular, for critical terms including "personal information" and "sensitive personal information" – and specific rights, such as the rights to know, correct, delete, and obtain a portable copy of their personal data; to opt out of its sale; and so on – that apply equally to any entity that interacts with consumer data would go a long way toward improving the process by which consumers are educated and empowered.

At the same time, businesses need a straightforward regulatory environment in which to innovate and operate that unambiguously defines a single set of reasonable obligations that apply nationwide. In contrast, overly burdensome restrictions on the use of consumer data disregard the win-win possibilities enabled by the willing transfer of personal information. Unnecessarily complicated requirements impose unwarranted compliance costs, costs that currently are compounded by a 20-state (and counting) "patchwork" of inconsistent and contradictory state-specific statutes. And the threat of frivolous lawsuits likely to benefit only the plaintiffs' bar deters innovation, investment, and marketplace entry. Such regulatory missteps ultimately harm competition, especially from small and upstart businesses, and, in turn, restrain consumer welfare.

Achieving equilibrium between these two sides is essential to maximizing efficiency. It also is a tall task, one that absolutely cannot be accomplished in a piecemeal manner. The creation of the seven-state Consortium of Privacy Regulators referenced above corroborates this conclusion: in banding together, these states have acknowledged that the existing "patchwork" approach is too unwieldy, even for regulators.

Instead, a federal comprehensive data privacy statute is needed that preempts all inconsistent state-level laws. I first made this point in "Inconsistent State Data Privacy Laws Increase

Confusion and Costs," a 2021 *Perspectives*. Others made similar arguments in their responses to the RFI.

For example, CTIA in its comments wrote that "[t]he existing patchwork of privacy frameworks increases the complexity and costs of compliance, unnecessarily straining private sector resources. This disjointed approach ultimately stymies innovation by diverting resources away from research and development."

The Computer & Communications Industry Association (CCIA) made the salient point that "internet-based services are inherently, and almost universally, interstate concerns which fall within the federal government's purview. State laws attempting to govern internet-based services can cause, in addition to the problems of consumer confusion and multiplied costs of compliance, an undue burden on interstate commerce."

USTelecom – The Broadband Association wrote that "[u]niformity … should be a paramount objective" and "[b]y establishing a clear, harmonized national framework, Congress can eliminate the growing patchwork of state and technology-specific laws, enable trusted data practices, and unlock the full potential of AI-driven transformation made possible by advanced broadband networks.

With respect to AI, the national security concerns surrounding AI compound the need for a uniform, nationwide approach to the regulation of AI rather than the balkanized approach foretold by Colorado's first-in-the-nation Senate Bill 24-205, which became law in June 2024. As just one example, an April 2025 report prepared by the House Select Committee on the CCP characterized the DeepSeek AI chatbot as "a profound threat … [that] siphons data back to the People's Republic of China (PRC), creates security vulnerabilities for its users, and relies on a model that covertly censors and manipulates information pursuant to Chinese law."

As CTIA noted in its RFI response:

> It is the policy of the United States to 'sustain and enhance America's global AI dominance," [and] [s]tate privacy laws that seek to constrain AI not only create a fragmented regulatory environment, but also risk imposing significant burdens on businesses, potentially slowing the pace of AI innovation in the United States…. AI-specific provisions in state privacy laws are unnecessary, would have negative impacts on innovation and U.S. leadership, and would stand to quickly become outdated given the rapid evolution of this technology. (citation omitted)

IV. The Application of Privacy Regulations Should Hinge Upon the Activity at Issue, Not the Identity of the Entity Involved

Businesses interacting with consumer data in similar ways should be treated similarly. Consumers generally aren't privy, say, to the different regulatory classifications applied by the FCC to communications providers versus others with whom they compete in the broader online ecosystem. Nor should they need to be.

Instead, and as CTIA wrote in its comments:

> To avoid confusion over which body is responsible for enforcing which laws, federal privacy legislation should also preempt FCC authority over consumer privacy and data security. Today's split enforcement regime, where both the FCC and FTC enforce data privacy and security regulations, creates consumer confusion and is inefficient. This is not useful, as consumers do not expect their privacy rights to differ based on regulatory arcana or platform characteristics. (citation omitted)

Similarly, USTelecom pointed out that, "[u]nder current law, communication providers are subject to a separate body of privacy regulations, which in some instances vary by service category, as well as further regulation by the FCC. A new federal privacy framework should supplant that separate body of regulations."

V. Exclusive Enforcement by the FTC Would Put the Interests of Consumers First

The way that a federal comprehensive data privacy statute is enforced presents yet another potential threat to the bedrock principles of consistency and clarity. As I explained in "A Privacy Private Right of Action Is Inferior to FTC Enforcement," a January 2020 *Perspectives*, placing exclusive enforcement in the hands of the FTC ensures a single, harmonized set of statutory interpretations and the imposition of remedies narrowly tailored to discouraging the problematic activity and/or making injured consumers whole. A private right of action, by contrast, threatens yet another "patchwork," in this case inconsistent or contradictory decisions made in different judicial venues.

Of greater concern, the inclusion of a private right of action would incentivize costly litigation untethered to actual consumer harm. As the Council for Citizens Against Government Waste (CCAGW) argued in the RFI comments:

> To avoid excessive and frivolous litigations, Congress should not include a private right of action (PRA) in any law related to consumer data privacy and security. A PRA allows trial lawyers to act in an enforcement capacity by bringing suits against a business where they deem that there could be a violation of the law and seek monetary restitution. According to the U.S. Chamber of Commerce Institute for Legal Reform, "PRAs can lead to litigation abuse because plaintiff's lawyers are financially incentivized to file as many lawsuits as possible, placing monetary gain over properly addressing potential harms. Unfortunately, private rights of action do not enhance consumer privacy or protection but rather serve the interests of plaintiffs' lawyers seeking large payouts. (citation omitted)

VI. Conclusion

With each new Congress, one can find reasons to be cautiously optimistic that, this time, a comprehensive data privacy bill at long last will pass. In this instance, I am encouraged by the decision to create a dedicated working group, the choice to start with a call for public input, and the overall tenor of the RFI. Now lawmakers should reach agreement on statutory language that defines clear and consistent rights for consumers and responsibilities for companies, strikes the appropriate balance essential for responsible innovation in the online ecosystem, and 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 Potomac, 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, "House Commerce Privacy Working Group Seeks Input," *FSF Blog* (March 4, 2025).

Andrew Long, "House Commerce Leaders Create Privacy Working Group," *FSF Blog* (February 18, 2025).

Andrew Long, "Michigan Could Become State No. 21 to Pass a Data Privacy Law," *FSF Blog* (December 17, 2024).

Andrew Long, "2024 Data Privacy Legislative Review: Federal Lawmakers Fall Short As More State Laws Gain Teeth," *Perspectives from FSF Scholars*, Vol. 19, No. 44 (December 13, 2024).

Andrew Long, "Will AI Help or Hinder Federal Privacy Legislative Efforts?" *FSF Blog* (July 16, 2024).

Andrew Long, "Federal Privacy Bill Hits Roadblock, State Activity Picks Up Speed," *FSF Blog* (June 28, 2024).

Andrew Long, "Congressional Leaders Return Privacy to the Front Burner," *Perspectives from FSF Scholars*, Vol. 19, No. 13 (April 19, 2024).

Andrew Long, "More States Compound the Dreaded Privacy 'Patchwork' Problem," *Perspectives from FSF Scholars*, Vol. 18, No. 31 (July 24, 2023).

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

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