Perspectives from FSF Scholars
September 23, 2022
Vol. 17, No. 48

Expanding Cracks Threaten the Privacy Preemption Legislative Compromise

by

Andrew Long *

I. Introduction and Summary

Recent developments – the long-signaled initiation of a rulemaking by the FTC, the adoption by five states of incompatible comprehensive data privacy laws, and the enduring, undeniable need for a privacy regime that embodies uniform, technology and location neutral consumer rights and corporate responsibilities – have increased the pressure on Congress to act on data privacy. Pressure alone, however, cannot bridge deep-rooted differences, particularly those involving the preemption of rival statutes at both the state and federal levels.

The American Data Privacy and Protection Act (ADPPA), first introduced as a Discussion Draft and then passed by a near majority of the House Commerce Committee as an amendment in the nature of a substitute (AINS), reflects the intense desire of lawmakers from both political parties to drive the legislative process forward. Stepping back, though, it is impossible to ignore the potentially fatal cracks that exist below the celebrated surface-level compromise. Absent a true reconciliation of the fundamental differences that exist, a sound policy approach that addresses the interests of American consumers will remain out of reach.

As a practical matter, the Discussion Draft, introduced on June 3, 2022, by a bipartisan and bicameral group of leaders, represented a tenuous, perhaps unworkable, compromise on preemption: broad language preempting state laws offset by a laundry list of exceptions threatening to swallow the rule. Changes reflected in the AINS further heightened that tension, especially regarding the role of California's first-of-its-kind state privacy agency. Recent indications from Speaker of the House Nancy Pelosi, meanwhile, seem to suggest that *any* attempt to preempt state efforts in this sphere may be a cause for blocking additional forward momentum. As the rubber meets the road, it appears that there is much less substance to the ADPPA's claimed compromise on preemption than initially hoped.

Lest we forget, a primary promise of a federal comprehensive data privacy law is a regime that, via consistent and uniform application, provides consumers with the simplicity, clarity, and transparency that some argue today's "notice and consent" approach lacks. The preemption of inconsistent, rival state laws is an essential component thereof.

Another critical feature to which consumers are entitled is the even-handed treatment of their personal information solely based upon the nature of that data, without regard to legacy, siloed regulatory categorizations that lack relevance in 2022. On this point, changes wrought by the AINS improve upon the Discussion Draft by preempting the FCC's oversight of certain communications services and replacing it with uniform, bolstered FTC authority over all such offerings, no matter who provides them. Regrettably, certain commenters, chief among them Public Knowledge, instead cling to an Analog Era, telephone-grounded model that is wholly incompatible with the modern, technology neutral regime that is the appropriate foundation for federal legislation in the Digital Age.

Consumers deserve simple and easy to understand data privacy safeguards dictated exclusively by the nature and sensitivity of the personal information involved – not where they or the provider is located or how that provider may have been regulated prior to the long-awaited establishment of a revolutionary, modern approach to data privacy. Lawmakers on both sides of the aisle cannot lose sight of that fact if the ADPPA is to become an effective law grounded in today's digital marketplace realities.

II. State-Specific Carve-Outs Are Inconsistent With a Uniform Privacy Regime

A primary motivation driving the ADPPA forward thus far is the proliferation of incompatible, state-specific data privacy statutes. In order to sidestep the consumer confusion and commercial costs that such laws – which to date have been passed in five states – inevitably will cause, it is critical that any federal law preempt state-specific statutes.

As I noted in "Bipartisan Privacy Discussion Draft: Significant, If Incomplete, Progress," a June 2022 *Perspectives from FSF Scholars*, the Discussion Draft helpfully included broad preemptive language. However, exceptions to that general rule, in the form of carve-outs for specific state statutes, undermined its overall thrust.

The AINS exacerbates that shortcoming by expanding the extent to which California may forge its own path. Whereas the Discussion Draft merely exempted that state's limited private right of

action for certain security breaches, the AINS broadly empowers the California Privacy Protection Agency to "enforce [the ADPPA], in the same manner, it would otherwise enforce the California Consumer Privacy Act." The authority of the California Privacy Protection Agency CPPA), created by the California Privacy Rights Act, includes the right to investigate possible violations, conduct hearings, issue cease and desist orders, impose fines, and adopt rules. The AINS' expansion of this exception to FTC enforcement for the CPPA effectively revives the problem of disparate consumers rights based upon geographic location that a preempting federal law otherwise would solve. Given California's size and prominent role in the digital economy, the potential ramifications of this change to the Discussion Draft are substantial.

What's more, Speaker of the House Pelosi at the beginning of this month issued a statement advocating for even greater deference not only to her home state's privacy statutes, but seemingly to state laws across the board: "it is imperative that California continues offering and enforcing the nation's strongest privacy rights … states must be allowed to address rapid changes in technology."

In other words, the imperfect consensus on state preemption achieved in the Discussion Draft appears to rest on increasingly shaky ground. Moving forward, lawmakers should remove state-specific carve-outs from the ADPPA and limit the role of the states to enforcement of uniform, nationally applicable protections by their attorneys general – as well as, perhaps, California's CPPA.

III. A 21st Century Approach to Data Privacy Demands Technological Neutrality

In addition to geographic uniformity, consumer clarity requires that products and services be regulated in an even-handed fashion based upon the nature and sensitivity of the data at issue, rather than the legacy regulatory classification of the provider or the identity of the agency, here the FCC, that happened to enforce that legacy regulatory classification. With respect to communications offerings, that means that individuals should have confidence that their interactions – whether via video, voice, or text – are protected in the same manner, based on the nature and sensitivity of the data at issue, no matter who moves that data from point A to point B. The AINS accomplishes this through a two-step, clean-slate approach.

First, recognizing that today entities of all stripes provide communications services that once were available exclusively from those subject to the authority of the FCC, the AINS substitutes FTC enforcement for the FCC's legacy privacy regulations:

> Notwithstanding any other provision of law, sections 222, 338(i), and 631 of the Communications Act of 1934 …, and any regulations and orders promulgated by the Federal Communications Commission under any such section, do not apply to any covered entity with respect to the collection, processing, transfer, or security of covered data or its equivalent, and the related privacy and data security activities of a covered entity that would otherwise be regulated under such sections shall be governed exclusively by the provisions of [the ADPPA], ….

Second, it defines as "sensitive covered data" the following comprehensive list of services, without regard to who provides them:

> An individual's private communications such as voicemails, emails, texts, direct messages, or mail, or information identifying the parties to such communications, voice communications, video communications, and any information that pertains to the transmission of such communications, including telephone numbers called, telephone numbers from which calls were placed, the times calls were made, call duration, and location information of the parties to the call, ….

This technology agnostic approach accurately reflects the myriad ways in which Americans in 2022 communicate with one another – think Meta's Facebook Messenger, WhatsApp, and Instagram; Google Hangouts and Chat; Apple Messages and Facetime; Zoom; Slack; Snapchat; and so on. And it provides consumers with clear rules of the road that apply based upon the type of data involved, not the legacy regulatory classification of the provider or the agency that happened to enforce that legacy regulatory classification.

In addition, the AINS takes significant steps to ensure the effectiveness of the FTC's exclusive oversight, including by expanding its rulemaking authority and establishing a new Privacy Bureau.

Shortly after the AINS was voted out of the House Commerce Committee, however, a Public Knowledge blog post took issue with its modern, uniform approach, dismissively asserting that "your most intimate phone details will now be protected by the Federal Trade Commission under a scheme designed for your Amazon ordering history and your Facebook 'likes.'" This characterization understates grossly both the amount of consumer data to which Big Tech has access and the extent to which Americans rely upon the Internet-based communications services that they provide.

Public Knowledge attempts to generate support for its position by suggesting that the AINS's preemption of Section 222 "with respect to the collection, processing, transfer, or security of covered data or its equivalent, and the related privacy and data security activities of a covered entity that would otherwise be regulated under such sections" might have negative consequences for voice competition. However, the AINS on its face does not appear to implicate the provisions in Section 222 relating to number portability – a fact that Public Knowledge seems to concede ("Under Section 203 of the ADPPA… not so much, or at least *maybe* not so much" (emphasis in original)). And to the extent that this is a legitimate concern, it could be addressed through targeted, tightly drawn edits.

IV. Conclusion

Bipartisan congressional efforts to advance the ADPPA reflect the increasingly pressing need for a national data privacy regime. However, steady efforts to chip away at the fragile, flawed compromise on preemption accomplished by the Discussion Draft threaten to flatten the ADPPA's tires well short of the finish line. One virtue of a federal data privacy law is that, unlike state-specific statutes, it can provide consumers with consistent and easy to understand

protections that apply throughout the country. In addition, a federal approach can base those rights exclusively on the nature of the personal information involved through the elimination of the FCC's legacy rules rooted in the Analog Era. As lawmakers continue to refine the ADPPA's text, they should remain focused on the important role that preemption, in both of these forms, can play in providing consumers with the uniform, understandable approach they deserve.

* 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 From the Author

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

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

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

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

"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).

"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).

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

"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 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).