Perspectives from FSF Scholars
December 4, 2019
Vol. 14, No. 42

Federal Privacy Legislation: Bipartisan Discussions Devolve into Dueling Drafts

by

Andrew Long *

Time is running short for Congress to act on privacy. The holiday recess begins in less than two weeks and, absent the passage of a preemptive federal bill, the California Consumer Privacy Act ("CCPA") may become the *de facto* law of the land on January 1, 2020.[1] The Senate Commerce Committee is holding a hearing on Wednesday, December 4, 2019[2] – but bipartisan discussions, once seen as a promising path forward, have failed to produce results.[3]

[1] In a recent blog post, I explain why businesses are likely to apply the requirements of the CCPA nationwide. *See* "California's Privacy Law: Recent Developments Underscore the Need for Preemptive Federal Law," (November 21, 2019), available at https://freestatefoundation.blogspot.com/2019/11/californias-privacy-law-recent.html. And in an October 2019 *Perspectives*, I offer a broad critique of the CCPA itself. *See* "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), available at https://freestatefoundation.org/wp-content/uploads/2019/10/California's-Heavy-Handed-Approach-to-Protecting-Consumer-Privacy-–-Exhibit-A-in-the-Case-for-Federal-Preemption-102819.pdf.

[2] *See* Press Release, "Committee Announces Hearing on Consumer Data Privacy," (November 25, 2019), available at https://www.commerce.senate.gov/2019/11/committee-announces-hearing-on-consumer-data-privacy. Scheduled witnesses include representatives from Microsoft, the 21st Century Privacy Coalition, the Georgetown Law Center on Privacy & Technology, Walmart, and the Center for Democracy and Technology.

[3] *See, e.g.*, Cameron F. Kerry, "Senate Democratic privacy principles: Endgame or game over for a bipartisan bill?," *Brookings*, (November 22, 2019), available at

Senators from the two parties appear unable to reach consensus regarding two fundamental issues: (1) whether individual consumers should have the right to sue companies for alleged violations, and (2) whether states should be able to impose their own regulations that go further than what is required under federal law. Democrats support both – and maintain that, at a minimum, federal law must allow for the former. Republicans disagree.

Until fairly recently, Senators were debating these points behind closed doors. With the year's end rapidly approaching, however, Senate Democrats have made their positions known. On November 18, ranking members of the Commerce (Maria Cantwell (WA)), Judiciary (Dianne Feinstein (CA)), Banking (Sherrod Brown (OH)), and Health, Education, Labor and Pensions (Patty Murray (WA)) Committees released a set of core principles that they believe should inform any eventual legislation.[4] And on November 26, four Democratic members of the Commerce Committee – Maria Cantwell, Brian Schatz (HI), Amy Klobuchar (MN), and Ed Markey (MA) – introduced the Consumer Online Privacy Rights Act ("COPRA").[5] In response, Commerce Committee Chair Roger Wicker (MS) reportedly has circulated a staff discussion draft that sets forth Republicans' rival positions.[6]

COPRA is comprehensive in scope. Among other things, it would establish an expansive array of consumer privacy rights; broadly define the category of personal information for which "opt-in" consent is required; create a "duty of loyalty"; direct covered entities to conduct annual discrimination-focused assessments of their algorithmic decision-making processes; require senior executives to certify compliance; protect whistleblowers; establish a new FTC bureau; and address digital content forgeries ("deepfakes"). And of particular concern, it would create an individual private right of action and decline to preempt state law. To its credit, however, COPRA would not distinguish between Internet service providers ("ISPs") and so-called "edge" providers, treating both as "covered entities."[7]

Consumers would suffer harm if COPRA were to become law. They expect their privacy to receive consistent protection no matter where they, or the businesses with which they transact, are located. COPRA would frustrate that expectation. They also enjoy the benefits that they receive from "free," data-driven offerings. COPRA's overreaching constraints on businesses'

---

https://www.brookings.edu/blog/techtank/2019/11/22/senate-democratic-privacy-principles-endgame-or-game-over-for-a-bipartisan-privacy-bill/ ("Members of a Senate Commerce group have been working on a bipartisan basis for over a year to come up with a bill to provide baseline privacy protections – but they have yet to issue any proposal.").

[4] *See* "Privacy and Data Protection Framework," (November 18, 2019), available at https://www.democrats.senate.gov/imo/media/doc/Final_CMTE%20Privacy%20Principles_11.14.19.pdf (announcing privacy principles designed to "establish data safeguards," "invigorate competition," "strengthen consumer and civil rights," and "impose real accountability").

[5] *See* Press Release, "Senate Democrats Unveil Strong Online Privacy Rights," (November 26, 2019), available at https://www.commerce.senate.gov/2019/11/senate-democrats-unveil-strong-online-privacy-rights.

[6] *See* Daniel R. Stoller, "Federal Privacy Law Would Override States Under Draft Plan," *Bloomberg Law*, (November 29, 2019), available at https://news.bloomberglaw.com/privacy-and-data-security/federal-privacy-bill-would-override-states-under-draft-language (reporting that the staff discussion draft "would prevent states from enforcing data privacy or security laws that would affect companies covered by the proposal" and "doesn't include a private right of action").

[7] However, it would not eliminate Federal Communications Commission jurisdiction over telephone, cable, and Direct Broadcast Satellite ("DBS") subscriber privacy. Thus, the playing field would remain at an angle.

ability to use personal information, additional costs, and litigation risks would jeopardize existing offerings, threaten innovation, and discourage new entry.

No Preemption of State Laws: The digital services marketplace knows no state boundaries. Federal privacy law holds the potential to benefit consumers through the establishment of a single set of rules, consistent with what individuals expect when they go online. Exclusive federal oversight also shields consumers from the costs that businesses would incur to comply with a "patchwork" of state regimes. COPRA, however, expressly does *not* preempt state action that "affords a greater level of protection to individuals protected under this Act."[8]

An Individual Private Right of Action: Exclusive enforcement by the Federal Trade Commission and state attorneys general would safeguard consumer privacy rights without unreasonably interfering with the efficient operation of the marketplace. By contrast, COPRA would permit "[a]ny individual alleging a violation of this Act or a regulation promulgated under this Act [to] bring a civil action in any court of competent jurisdiction, State or Federal"[9] and authorize remedies up to "$1,000 per violation per day or actual damages, whichever is greater," as well as punitive damages.[10] COPRA's inclusion of a private right of action would threaten continued investment in digital services. It also could prompt businesses to reevaluate the viability of "free" content and services fueled by personal information, resulting in consumers having to pay for that which they enjoy today at no cost.

The possibility of private litigation distorts incentives and produces unintended negative consequences. In other words, it encourages consumers to go to court – and lawyers to take on those cases. Individual law suits also burden the public-funded judicial system and redirect corporate resources away from uses that generate consumer welfare. COPRA includes a litany of privacy rights for consumers and responsibilities for businesses, many of which are defined using ambiguous language. (For example, the "duty of loyalty" broadly states that covered entities may not "engage in a deceptive data practice," a term that, notwithstanding reference to Section 5 of the Federal Trade Commission Act, inevitably invites multiple interpretations.[11]) Each one of these entitlements and liabilities would expose businesses to potential risk. That risk, in turn, would harm consumers by discouraging existing providers from continuing to offer data-driven services and investing in innovative new offerings – as well as undermining incentives for new participants to enter the marketplace.

Overreaching Consumer Privacy Rights: Consumer privacy rights, reasonably defined, include transparency into businesses' data collection practices; the ability to view, correct, delete, and download the data that businesses collect; and the right to "opt-out" of the sale of personal information to third parties. By contrast, COPRA would go much further, creating additional entitlements with respect to data minimization and security[12] as well as the aforementioned "duty of loyalty." Unreasonably broad and vaguely defined rights invite

[8] Consumer Online Privacy Rights Act § 302(c), (November 26, 2019), available at https://www.cantwell.senate.gov/imo/media/doc/COPRA%20Bill%20Text.pdf (*COPRA*).
[9] *COPRA* § 301(c)(1).
[10] *COPRA* §§ 301(c)(2)(A), (B).
[11] *COPRA* §§ 101(a)(1), (b)(1).
[12] *See COPRA* §§ 106, 107.

gratuitous litigation, the potential costs of which reduce covered entities' incentives to take welfare-generating risks.[13]

In addition, the broad definition of "sensitive covered data" for which "opt-in" consent is required includes browsing history – *i.e.*, "[i]nformation revealing online activities over time and across third-party websites or online services."[14] Imposing an "opt-in" consent requirement for all browsing information would disrupt the existing digital services marketplace and jeopardize the continued viability of the "free" content and services that consumers value.

Reporting from late last week,[15] however, indicates that Senate Commerce Committee Chairman Wicker has responded to Democrats' public line-drawing with a staff discussion draft spelling out Republicans' opposing views.[16] Entitled the United States Consumer Data Privacy Act ("USCDPA"), it deviates from COPRA in four significant ways:

- First, it doesn't create an individual private right of action, but rather solely empowers the FTC and state attorneys general to enforce its provisions through civil actions.[17]

- Second, it expressly preempts state data privacy laws, clarifying that "[n]o State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard related to the data privacy or security and associated activities of covered entities."[18]

- Third, it requires "opt-in" consent for browsing history only to the extent that that information itself falls within the definition of "sensitive covered data."[19]

- Fourth, it ensures a level playing field between ISPs and "edge" providers by (a) granting the FTC enforcement authority over "common carriers" subject to the Communications Act of 1934, as amended ("Communications Act"), and (b) preempting the Communications Act, and implementing rules adopted by the Federal Communications Commission, "with respect to the collection, use, processing, transferring, or security of consumer information."[20]

---

[13] The fact that COPRA excludes certain small businesses from the definition of "covered entity" itself acknowledges the bill's burdensome nature. *See COPRA* §§ 2(9)(C), (23).
[14] *COPRA* § 2(20)(J).
[15] *See* Daniel R. Stoller, "Federal Privacy Law Would Override States Under Draft Plan," *Bloomberg Law*, (November 29, 2019), available at https://news.bloomberglaw.com/privacy-and-data-security/federal-privacy-bill-would-override-states-under-draft-language.
[16] *See* Staff Discussion Draft, "United States Consumer Data Privacy Act of 2019," available at https://aboutblaw.com/NaZ (*USCDPA*).
[17] *See generally USCDPA* § 402.
[18] *USCDPA* § 404(a).
[19] *USCDPA* § 2(20)(J) (defining "sensitive consumer data" to include "[c]overed data about the online activities of an individual that relate to a category of covered data described in another subparagraph of this paragraph").
[20] Currently, the FCC has jurisdiction over telephone subscriber privacy under Section 222 of the Communications Act, 47 U.S.C. § 222, cable subscriber privacy under Section 551 of the Communications Act, 47 U.S.C. § 551, and Direct Broadcast Satellite ("DBS") subscriber privacy under Section 338 of the Satellite Home Viewing Improvement Act, 47 U.S.C. § 338.

From a policy and legal perspective, the USCDPA represents a meaningful improvement on COPRA. While the few remaining days on the legislative calendar before the holiday recess represent a rapidly closing window for bipartisan collaboration, Congress nevertheless should try to pass federal privacy law that preempts individual state laws. If it fails to do so prior to January 1, as a practical matter, the CCPA presumably will fill that void.

* Andrew Long is an Adjunct Senior Fellow of the Free State Foundation, an independent**,** nonpartisan free market-oriented think tank located in Rockville, Maryland.