

Policy Backgrounder: Data Privacy Legislation

June 28, 2024

Trusted Insights for What's Ahead™

CED's recent Solutions Brief [Principles for AI Guardrails in the US](#) noted that “[d]ata privacy is a foundational pillar of responsible AI development. However, the US currently lacks a federal statutory or regulatory framework governing the collection and usage of personal data.” Congress is actively considering two bills that aim to provide that framework, one comprehensively and one focused on children but face strong opposition, including from many technology companies.

- Unusually, the House Energy and Commerce Committee [canceled](#) at the last minute a scheduled committee markup including the two data privacy bills: the proposed [American Privacy Rights Act](#) (APRA) and the [Kids Online Safety Act](#) (KOSA) on June 27.
- APRA has some bipartisan support but faces strong opposition in its current form from both technology companies and some Congressional leaders, making the path to enactment potentially very difficult. KOSA has strong bipartisan support, particularly in the Senate.
- Solicitor General Vivek Murthy's recent [call](#) for warning labels on social media also highlights issues surrounding the use of platforms, particularly with respect to children. But placing warning labels on social media are very unlikely.

The Two Bills

Background to the APRA

House Energy and Commerce Committee Chair Cathy McMorris Rodgers (R-WA), who is retiring after this Congress, has made passage of data privacy legislation a priority for her last term. Privacy advocates have long supported establishment of a US data privacy framework, noting the EU's [General Data Protection Regulation](#) (GDPR) and similar laws in some states including the [California Consumer Privacy Act](#). US companies with operations in the EU must comply with the GDPR; many US companies must comply with the California law or other similar state laws. Broadly, the GDPR gives individuals rights to access, correct, and delete inaccurate personal data and to limit companies' access to that data, not least by giving users the option to reject cookies used to collect data (the link to GDPR above from an official EU website is a good example of this in practice).

Major issues that would be considered in any comprehensive Federal data privacy framework include the extent of companies' responsibilities, the definition of sensitive data, the extent of consumers' opt-out rights, the role of data brokers, the extent of Federal preemption of state laws, the potential impact on small businesses, and who would have a right to sue under the framework.

American Privacy Rights Act

The [current](#) version of [APRA](#), which was scheduled for markup on June 27 before the cancellation of the hearing, resulted from an [agreement](#) between McMorris Rodgers and Rep. Frank Pallone (D-NJ), the ranking member of the committee. McMorris Rodgers also reached [agreement](#) with Senate Commerce Committee Chair Maria Cantwell (D-WA) on the [outlines](#) of data privacy legislation. The draft includes

Federal preemption of state data privacy standards (important for business), limitations on companies' ability to collect certain kinds of data, data security standards "to hold companies accountable if data is hacked or stolen," and permitting a private right of action by "persons" (which includes corporations as well as individuals) to bring lawsuits against "bad actors" for violations of privacy rights including those related to sensitive, biometric, or genetic information. The bill also gives state Attorneys General the right to sue for violations.

APRA includes these provisions, including the private right of action against "covered entities" (which exempts small business), limitations on what data technology companies can retain, and explicitly permitting consumers to opt out of targeted advertising (an important provision of the GDPR). It would also prohibit targeted advertisements to children under 17.

"Covered entities" include individuals, companies, and nonprofits that "alone, or jointly with others, determine[] the purposes and means of collecting, processing, and retaining, or transferring covered data." "Covered data" includes data that "identifies or is linked or reasonably linkable" to an individual person. "Sensitive covered data," which receives greater protection under APRA, includes information from government (for instance, drivers' license numbers and Social Security numbers) health, genetic, and biometric information; financial account numbers or other financial information; "precise geolocation information"; private communications (both numbers called and the content); and certain other types of sensitive information such as individuals' use of video programming.

The bill requires covered entities to [minimize](#) the data they collect to that "necessary, proportionate, and limited to provide or maintain . . . a specific product or service requested by the individual"; "a communication to the covered entity to the individual reasonably anticipated within the context of the relationship"; or one of [sixteen](#) permitted purposes, including market research, protection of data security, and compliance with legal and government obligations. Individuals would have a right to opt out of companies' transfer of covered data or its use for targeted advertising. Transfer of sensitive covered data would require express, affirmative consent from an individual.

Consumers would be able to access, correct, and delete their covered data held by a covered entity; covered entities would generally have 45 days to respond to user requests, though some large data holders (those with gross revenue over \$250 million) would have to respond within 30 days. The bill would also ban using "dark patterns" to harm individuals or retaliation against individuals for exercising data rights. Large data holders would be required to assess their algorithms' impact on privacy, and their CEOs would be required to certify compliance with APRA annually with the Federal Trade Commission (FTC). Other covered entities would be required to designate at least one privacy or data security officer.

The FTC would have principal enforcement responsibility under APRA, as it currently does with the [Children's Online Privacy Protection Act](#) (COPPA), deeming violations of APRA as "unfair or deceptive acts or practices" under the meaning of the [Federal Trade Commission Act](#). FTC could therefore [impose](#) civil penalties, injunctions, or other equitable relief for violations and could redistribute funds from monetary penalties to those affected by the prohibited conduct. The FTC could also issue regulations to further certain defined purposes of APRA, including defining sensitive covered data, data security, data minimization, and ensuring compliance. To promote enforcement, the bill would require establishment of a new FTC bureau in addition to its bureaus for Competition and Consumer Protection. FTC would set up a registry of data brokers and institute a Do Not Collect system along the lines of the Do Not Call system the FCC operates for telemarketing calls and a Delete My Data system applicable to data brokers, which must share a public website linking to the FTC's registry to permit the public to make requests to brokers.

Preemption of state laws is a focus of the bill. The preemption is fairly broad (states cannot "adopt, maintain, enforce, or continue in effect any law, regulation, rule or requirement covered by" APRA);

however, it exempts health information, employee information, and “consumer protection laws of general applicability”—all of which could serve as subjects for future litigation defining the scope of APRA.

Children’s Online Privacy Protection Act updates

The bill also revises COPPA, including a new prohibition on targeted advertising to minors, long a desire of privacy advocates. Currently, COPPA applies to children under 13 and only to online services that have “actual knowledge” they are collecting information from those children; it requires parental consent for collection or disclosure of data. APRA would expand this to prohibit transfer of sensitive covered data for children under 17 and prohibit “targeted advertising” to “covered minors” under 17, though without changing the “actual knowledge” standard under which the prohibition applies.

Finally, the bill is designed to complement, rather than replace, existing Federal privacy laws, including the [Gramm-Leach-Bliley Act](#) (financial services), the [Health Information Portability and Accountability Act](#), the [Fair Credit Reporting Act](#), the [Family Educational Rights and Privacy Act](#), and others. Covered entities would be “deemed” to be in compliance with APRA for most purposes if in compliance with those laws.

Kids Online Safety Act

[KOSA](#) also has bipartisan support. In the House, it was sponsored by Members including Reps. Gus Bilirakis (R-FL), Kathy Castor (D-FL), Erin Houchin (R-IN), Kim Schrier (D-WA), and Larry Bucshon (R-IN). The bill would require platforms to “exercise reasonable care” to avoid harms to children. It also includes greater provisions for parental controls on access to platforms and provisions on how companies in possession of minors’ personal data can use that data. A companion bill in the Senate introduced by Senators Richard Blumenthal (D-CT) and Marsha Blackburn (R-TN) has over 70 Senate cosponsors, including Senate Majority Leader Chuck Schumer. But Schumer is [reportedly](#) reluctant to bring the bill to the floor without an agreement that would limit time for debate, to save precious floor time as Congress approaches its August recess and to avoid spending time on a bill the House may not pass in any event.

House Markup Canceled

The canceled House Energy and Commerce Committee markup was scheduled at a time when there has been additional public attention on children’s online safety, notably a recent *New York Times* [article](#) on Meta focusing on material from a series of lawsuits brought by 45 states’ Attorneys General which are requesting stronger protections for minors on the platforms. The litigation schedules for the cases will likely proceed slowly; it seems clear, however, that at least some Attorneys General want to take personal testimony from Meta Platforms Chairman and CEO Mark Zuckerberg; New Mexico’s Attorney General Raúl Torrez [said](#) that “[a] lot of these decisions ultimately landed on Mr. Zuckerberg’s desk. He needs to be asked explicitly, and held to account explicitly, for the decisions that he’s made.” At this point in the litigation, it is unclear whether a court would require Zuckerberg’s testimony or whether this is an attempt to encourage settlement of the cases.

More broadly, the politics of APRA support are somewhat unusual. Some more liberal privacy advocates and some conservatives such as the [Heritage Foundation](#) have endorsed the bill, but it faces strong [opposition](#) from many technology companies ([Microsoft](#) is an exception) and other businesses including large online advertisers [led](#) by the National Retail Federation, the Association of National Advertisers, and the American Association of Advertising Agencies. (The National Federation of Independent Businesses supports the bill’s exemption of small business.) This opposition could make ultimate passage in the House difficult, even if the bill eventually receives a committee vote.

More specifically, House Speaker Mike Johnson (R-LA) and Majority Leader Steve Scalise [reportedly](#) opposed consideration of the bill at this time; without at least some level of support from the Speaker, he

could use his power to block consideration on the House floor even if the committee voted in favor of it. This opposition, after a [reported](#) meeting with Energy and Commerce Committee Republicans on Wednesday evening, likely led to cancellation of the markup.

Surgeon General Calls for Social Media Warning Labels

Surgeon General Vivek Murthy's recent call for warning labels on social media platforms may influence the debate over KOSA. Murthy argued that "social media is associated with significant mental health harms for adolescents. [A warning label] would regularly remind parents and adolescents that social media has not been proved safe . . . warning labels can increase awareness and change behavior." Any warning labels would require Congressional action. The proposal is not in KOSA, however, and it seems unlikely that Congress would adopt the idea, which technology groups [oppose](#).

Conclusion: Uncertain Prospects

There are several reasons why Congress might wish to adopt a comprehensive data privacy framework: Federal preemption of conflicting state laws (which could help provide certainty for business), the challenge of dealing with foreign standards such as the GDPR, and the increasing use of data to train AI models. Even if advances in generative AI were not proceeding at a rapid pace, Congress would likely still be considering data privacy legislation. But it is unclear at best whether either bill will eventually be considered on the House floor this session, not least because the Speaker has a very strong role in controlling the floor agenda absent a discharge petition requiring floor consideration. Another possible outcome is enactment of KOSA after a very strong Senate vote in favor, putting greater pressure on the House to act.

Even if APRA did pass, however, the path forward would not be simple. The FTC would have to adopt regulations, which could themselves be subject to legal challenges, and the bill would likely lead to major litigation as plaintiffs seek to expand or constrict its terms. Legal challenges could address both First Amendment free speech rights generally and commercial speech, a separate area of First Amendment jurisdiction with its own precedents.

About the Authors

[John Gardner](#) is Vice President, Public Policy at the Committee for Economic Development, the public policy center of The Conference Board.

About The Conference Board

The Conference Board is the member-driven think tank that delivers Trusted Insights for What's Ahead™. Founded in 1916, we are a non-partisan, not-for-profit entity holding 501 (c) (3) tax-exempt status in the United States. www.ConferenceBoard.org

The Committee for Economic Development (CED) is the public policy center of The Conference Board. The nonprofit, nonpartisan, business-led policy center delivers trusted insights and reasoned solutions in the nation's interest. CED Trustees are chief executive officers and key executives of leading US companies who bring their unique experience to address today's pressing policy issues. Collectively, they represent 30+ industries and over 4 million employees. www.ConferenceBoard.org/us/committee-economic-development

© 2024 The Conference Board, Inc. All rights reserved.