SQUIRE PATTON BOGGS

Privacy World

Keeping you informed on the evolving law on data privacy, security and innovation.

April's APRA: Could Draft Privacy Legislation Blossom into Law in 2024?

By Julia Jacobson, Alan Friel, Beth Goldstein, Kyle Dull, Stacy Swanson, Glenn A. Brown, John Wyand, Sasha Kiosse & Kyle Fath on April 11, 2024

This week, House Committee on Energy and Commerce Chair Cathy McMorris Rodgers (R-WA) and Senate Committee on Commerce, Science and Transportation Chair Maria Cantwell (D-WA) unveiled their bipartisan, bicameral discussion draft of the ***American Privacy Rights Act*** (APRA draft).**[1]** Chair Rodgers' and Chair Cantwell's announcement of the APRA draft surprised many congressional observers after comprehensive privacy legislation stalled in 2022.

In an interview, Chair Rodgers stressed, "**This is a discussion draft that Sen. Cantwell and I hammered out, but we're still open to constructive feedback**." The APRA draft, which could be introduced formally in the near term, reinvigorates congressional debates on national privacy protections. Advocacy around the APRA draft is expected to set off "**a huge lobbying bonanza**."

Meanwhile, critics of the APRA draft are emerging from among industry participants, consumer advocates, state privacy officials and lawmakers across the political spectrum. In addition to agreement on substantive issues, significant refinement of APRA's language is needed to minimize confusion and unintended consequences.

The following key questions discuss what entities and what data are covered by the APRA draft.

What data is protected in the APRA draft?

The APRA draft protects "covered data," which, like the definitions of personal information and personal data in the state consumer privacy laws, is broadly defined as information that "identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals." (Section 2(9)). Personal data collected and processed in a business-to-business context is not excluded from the APRA draft's definition of covered data. (To date, only California's state consumer privacy law applies to personal information collected in the business-to-business context).

An "individual" is a natural person "residing" in the United States (Section 2(24)) but not necessarily a U.S. citizen. Employees are not expressly excluded from the definition of individual but "employee information" is not covered data. (Section 2(9)(B)).

Several other data categories are excluded from the covered data definition, including de-identified data; publicly available information and inferences made exclusively from multiple independent sources of publicly available information that neither reveal sensitive covered data nor are combined with covered data; and research related information lawfully collected for a public library, archive, or museum.

The APRA draft includes an expansive definition for "sensitive covered data." The definition covers categories typically classified as sensitive under privacy laws, such as data that can be used for identity theft, health data, precise geolocation data, data from or about minors (under age 17) and data reflecting immutable personal physiological characteristics (i.e., biometric and genetic information, race). Data generally considered private, such as recorded media intended for "private use" or reflecting a "naked or undergarment-clad private area of an individual," data about an individual's video access and use transferred to a third party, and data in or about "private communications" also are sensitive covered data. The Federal Trade Commission (FTC) has the authority to expand the sensitive covered data definition via regulations.

What types of entities must comply with the requirements of the APRA draft?

The APRA draft follows the role-based model established in state and federal privacy laws: a covered entity determines the purposes and means of processing covered data as well as transferring covered data and a service provider processes or transfers covered data on behalf of, and at the direction of, a covered entity. The term "transfer" means sale or sharing of covered data for consideration or another "commercial purpose." (Section 2(42)). Whether an entity is a covered entity or service provider is a fact-based inquiry. The APRA draft does, however, impose more obligations on service providers than current state consumer privacy laws (e.g., more prescriptive data minimization and security obligations).

Of particular note, "common carriers subject to title II of the Communications Act of 1934" and nonprofit organizations are ***not*** exempt from the APRA draft and are thus subject to FTC enforcement in a stark departure from the FTC's Section 5 enforcement powers. (Section 17(b)(3)).

The APRA draft also regulates (i) data brokers, which are covered entities (but not service providers) that meet or exceed specified revenue thresholds related to processing or transferring covered data that the data broker did not collect directly from the individuals linked or linkable to processed or transferred covered data (Section 2(14)); and (ii) large data holders (LDHs), which are covered entities and service providers with at least $250m in gross revenue and that meet certain processing or transferring thresholds that seem targeted to social media platforms. One defined subset of LDH is a covered high-impact social media company (CHSMC), which is a covered entity that operates an internet-accessible platform (including its affiliates) that generates $3b or more in global annual revenue, has 300,000,000 or more monthly active users for at least 3 of the preceding 12 months; and is primarily used to access or share user-generated content.

Both data brokers and LDHs have enhanced transparency and compliance obligations.

Does the APRA draft have exemptions for entities subject to existing privacy laws?

The APRA draft does not contain *entity-level* exemptions for covered entities subject to existing federal privacy laws, such as for covered entities and their business associates subject to the Health Insurance Portability and Accountability Act (HIPAA) and financial institutions subject to the Gramm-Leach-Bliley Act (GLBA). Rather, the APRA draft offers two *information level* safe harbors:

> **Information Level Safe Harbor for Compliance with Certain Federal Privacy Laws**
>
> The APRA draft offers a compliance safe harbor "solely and exclusively with respect to any data" processed in compliance with the privacy requirements of the GLBA; Fair Credit Reporting Act; HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH); Social Security Act; Family Education Rights and Privacy Act (FERPA) (but only for a covered entity of service provider that is an educational agency or institution (as defined in FERPA)), among other laws set forth in Section 20(b)(3). The APRA draft requires the FTC to issue guidance regarding implementation of this privacy safe harbor within one year of APRA's enactment.
>
> **Information Level Safe Harbor for Compliance with Certain Federal Data Security Laws**
>
> The APRA draft offers a compliance safe harbor "solely and exclusively with respect to any data" that meets the information security requirements of GLBA, HITECH, Social Security Act and HIPAA. The APRA draft requires the FTC to also issue guidance regarding implementation of this data security safe harbor within one year of APRA's enactment.

The FTC's authority as to this part of Section 20 is to develop "guidance," as compared to rule-making in other Sections.

These two information-level safe harbors mean that many entities covered by entity-level exemptions in most of the current state privacy laws could face some significant new compliance challenges. But any non-compliance with "such laws and regulations" would seem to trigger application of APRA to a covered entity otherwise sheltered by a safe harbor, including the private right of action. The FTC implementation guidance may, however, introduce a narrower application.

What are the privacy rights available in the APRA draft?

Sections 5 and 6 offers a series of privacy rights like the state consumer privacy laws:

1. Right to access the individual's covered data and receive information about covered data transfers;

2. Right to correct the individual's covered data that is incorrect or incomplete;
3. Right to delete the individual's covered data processed by the covered entity and the covered entity's service provider;
4. Right to portability of the individual's covered data held by the covered entity;
5. Right to opt out of the transfer of the individual's covered data; and
6. Right to opt out of the use of the individual's covered data for targeted advertising.

These rights are subject to certain required exceptions (e.g., inability to verify, reasonable belief of fraud or crime, threat to security, violation of law or professional ethics obligations, etc.) and permissive exceptions and limitations (e.g., honoring the right is "demonstrably impossible" for the covered entity "due to technology or cost" or when an individual can exercise the right as to "on-device data" through "clear and conspicuous on-device controls," protection of trade secrets and as necessary to perform a contract or honor a rights request). The FTC is empowered to promulgate additional permissive exceptions. But the opt-out rights for covered data transfers and processing for targeted advertising do not have required or permissive exceptions, nor is the FTC empowered to develop any. Correction and deletion requests must be passed down to service providers and third parties to which a covered entity has transferred covered data.

The FTC is required to promulgate regulations within two years after enactment to establish technical specifications and other requirements for the right to opt out of a covered data transfer and right to opt out of targeted advertising.

What obligations apply to entities in the APRA draft?

The APRA draft includes these main compliance obligations:

Data Minimization (Section 3): Both covered entities and service providers must process, retain and transfer covered data only as necessary and proportionate to the purpose for which it was collected. Section 3 includes a list of permitted purposes, qualified by the need to demonstrate necessity, proportionality and purpose limitation. One of the permitted purposes – transfer as part of merger or other asset transfer – is more restrictive than under the state consumer privacy laws because it requires prior notice and the opportunity to withdraw previously given consent and/or request deletion for each individual.

Transfers of sensitive covered data are permitted only with affirmative express consent. The processing, retention and transfer of biometric and genetic information (a subset of covered sensitive data) also requires affirmative express consent (along with some other specific

obligations). The term "affirmative express consent" requires clear individual "authorization for an act or practice" in response to a "specific request" from a covered entity or from a service provider on its behalf after providing to the individual a clear and conspicuous standalone disclosure about the specific act or practice for which authorization is sought. (Section 2(1)).

The means for withdrawing affirmative express consent must be clear, conspicuous and as easy to use as the giving of affirmative express consent.

Transparency, Dark Patterns Prohibition (Section 4, Section 7): Both covered entities and service providers must publish privacy policies that meet the robust content requirements of Section 4(b), including specifically naming all data brokers to which covered data is transferred and the categories of other third parties and of service providers receiving covered data. One notable addition to the content requirements as compared to the state consumer privacy laws is the requirement to disclose whether any covered data collected by the covered entity or service provider is "transferred to, processed in, retained in, or otherwise accessible to a **foreign adversary**." A covered entity (but not a service provider) must provide advance "direct notification" of any "material change" to a privacy policy and allow individuals to opt out of the application of the material change to previously collected covered data. The (rather unhelpful) definition of "material change" is "with respect to treatment of covered data, a change by an entity that would likely affect an individual's decision to provide affirmative express consent for, or opt out of, the entity's collection, processing, retention, or transfer of covered data pertaining to such individual." An LDH also must publish a "short-form notice to consumers" not to exceed 500 words. Content requirements for short form notices are to be defined in FTC regulations.

A covered entity also is expressly prohibited from using dark patterns to divert an individual's attention from any privacy policy or notice, impair an individual's ability to exercise privacy rights or to obtain, infer, or facilitate an individual's consent for any action that requires an individual's consent. A dark pattern is defined as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice," which tracks the **FTC's current definition**.

Managing Privacy Rights Requests (Section 5 (c)-(d)): Covered entities must verify the identity of individuals or their authorized agents who make privacy rights requests. An LDH or data broker has fifteen (15) days to respond to a request. All other covered entities have thirty (30) days.

Obligations related to Targeted Advertising: The APRA draft materially deviates from the prevailing approaches to targeted advertising under state consumer privacy laws and would disrupt the prevailing business models of U.S. publishers and advertisers through a complex

combination of opt-in and opt-out to practices that enable more relevant ads to consumers, which garner greater ad revenues than less relevant ads. Further, the breadth of the opt-outs to transfers potentially impacts even non-targeted ad practices such as measurement, conversion tracking and frequency capping. Though complex, the import of such a sea change merits a close look at the draft provisions.

First, the right to opt out of covered data transfers has no exceptions and thus could prevent basic advertising functions like the use of service providers to assist with non-targeted ad serving, measurement and frequency capping. However, this may be a drafting oversight since those activities, along with contextual advertising, are carved out of the definition of targeted advertising and would fall under the permitted processing purposes of covered entities and service providers under Section 3(d)(14). This could be fixed by adding, as state consumer privacy laws provide, that transfers to service providers for permitted processing purposes are exempt from opt-out to transfer. The lack of such an exception will disrupt the ability to use service providers far beyond advertising vendors.

Turning now to interest-based advertising, transfers of sensitive covered data require affirmative express "opt-in" consent (Section 3(b)(1)) and "information revealing an individual's online activities over time and across websites or online services … or over time on any website or online service operated by a covered high-impact social media company" (TA Data for simplicity's sake) is sensitive covered data. Processing any covered data for targeted advertising is, however, on an opt-out basis. (Section 6(a)(2)). The APTS draft defines Targeted Advertising as "displaying or presenting to an individual or device identified by a unique persistent identifier (or group of individuals or devices identified by unique persistent identifiers) an online advertisement that is selected based on known or predicted preferences or interests associated with the individual or device identified by a unique identifier."

So, the targeted advertising opt-out prohibits collection (a form of processing) of TA Data since its purpose is in furtherance of targeted advertising. Accordingly, the targeted advertising opt-out is both a withdrawal of consent to transfer, and a prohibition of collection of TA Data, as well as an opt-out of processing of any non-TA covered data to further targeted advertising, which would include non-TA Data used to supplement TA Data for targeted advertising.

The opt-out, though overly complex, is broader than some state consumer privacy laws but is consistent with their opt-out regime. However, the added opt-in for transfer of TA Data is a radical departure. Targeted advertising will be stymied by the need to get affirmative express consent to transfer of TA Data since the standard for that opt-in is "affirmative express consent" to permit the

covered entity that collected the applicable categories of data to transfer it. This may prove challenging as it has in Europe under the General Data Protection Regulation (GDPR).

It should be further noted that data minimization Section 3(a)(2) combined with 3 (d)(15) arguably seem to prohibit any processing of sensitive covered data (including TA Data) for targeted advertising outright, and only permit use of non-sensitive-covered-data for targeted advertising if not opted-out. That would be inconsistent with the concept of opt-in. However, if you look at subsection 3(a), it carves out subsections (b) (opt-in to sensitive covered data transfers) and (c). So, reading (a) and (b) together leads to a conclusion that opt-in is needed for transfer of sensitive covered information for targeted advertising, and that you can only use sensitive covered data for targeted advertising if you received it via a proper opt-in to the transfer (and, implicitly, there has been no subsequent opt-out), but you can use non-sensitive-covered-information for targeted advertising unless opt-out. Not well written, but otherwise, (a) and (d) are in conflict.

At any event, given the standard for affirmative express consent applied in the context of TA Data seems challenging to meet, publishers will have a harder time engaging in targeted advertising than under the current opt-out regime under state consumer privacy laws. This will impact their ad revenues that support many U.S. online service models and give us a largely free and open Internet. Further, the breadth of Section 8's prohibition on different prices or service levels based on rights exercise, other than in the context of a loyalty program or market research, threatens targeted-advertising-free paywalls (i.e., pay for privacy; "pay or ok"). This may result in more publishers being forced to charge all users some amount for access to offset ad revenue losses. This could further the digital divide for less affluent Americans.

Data Security (Section 9): Both covered entities and service providers must establish, implement and maintain data security practices. The data security requirements in the APRA draft are similar to the requirements in state data security laws (e.g., New York's **Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)**) but also contain six (6) specific requirements (Section 9(b)), including requirements for vulnerability assessments, retention schedules, destruction procedures and employee training. The FTC is required to enact regulations to interpret Section 9 in consultation with the Department of Commerce.

Data Privacy Officer (Section 10): A covered entity must designate one or more "qualified" employees to serve as privacy or data security officer(s). An LDH must designate a qualified privacy officer *and* a qualified data security officer, one of whom oversees development and maintenance of privacy and data policies, procedures and recordkeeping and employee training and conducts biennial compliance audits.

Obligations Specific to Service Providers and Third Parties (Section 11): A service provider is required to assist the covered entity in meeting the covered entity's APRA obligations. A covered entity must have a written contract with each service provider which contains terms that are similar to those in the state consumer privacy laws.

A third party is an entity that receives covered data from a covered entity, is not a service provider and is not under common control from the entity providing the covered data. A third party must only use the covered data for the purpose(s) for which the individual has received notice or, in the case of sensitive covered data, gave affirmative express consent. A third party may rely on the representations of the covered entity from which it receives the covered data after some "reasonable due diligence." A covered entity is not liable for APRA violations by a transferee of its covered data as long as the covered entity is in compliance with APRA requirements and did not have actual knowledge that the transferee intended to violate APRA.

Covered Algorithms (Section 13): A covered entity or service provider that knowingly develops a covered algorithm must evaluate "the design, structure, and inputs" of the covered algorithm, including any training data used to develop the covered algorithm, to reduce the risk of the specified potential harms.

Additional Obligations for LDHs and data brokers

An LDH must (inter alia) publish annual reports on its receipt and handling of privacy rights requests (Section 5(f)), file annual certifications about internal reporting structures and compliance controls (Section 10), conduct an annual privacy impact assessment (Section 10) and maintain logs of privacy policy changes (Section 22). Within two years after APRA's enactment, an LDH must conduct an impact assessment of its use of a "covered algorithm" in a manner that poses a "consequential risk" of harm. (Section 13).

Section 12 sets out a series of additional requirements applicable to data brokers, including requirements for transparent notices with language requirements to be developed by the FTC and an online tool for individuals to submit "do not collect" requests and exercise the other individual privacy rights in Sections 5 and 6 of the APRA draft. The FTC also is required to establish a federal data broker registry.

What existing laws are / are not pre-empted by the APRA draft?

State Preemption (Section 20(a))

The APRA draft generally preempts the sixteen (16) (to date) state general consumer privacy laws. The APRA does not, however, preempt the following categories of state laws:

- State consumer protection and contract law
- Employee privacy laws
- Student privacy laws
- Data breach notification laws (in all 50 states)
- Provisions of laws that address electronic surveillance, wiretapping and telephone monitoring (see, e.g., here)
- Laws that address social security numbers, identify theft, credit reporting, banking records, financial records and tax records, among others described in Section 20(a)(3)(k)
- Laws related to unsolicited marketing email sand telephone calls
- Civil rights and sexual harassment laws
- Laws related to stalking, cyberstalking, cyberbullying, sexual harassment, child abuse and trafficking
- Laws that protect the privacy of health, healthcare and medical information, medical records, HIV status or HIV testing." (Preemption exemption suggests that all or some of Washington's My Health My Data (**read more**) and other state consumer health data laws are not preempted)

Federal Preemption

At the federal level, the APRA draft makes clear that the APRA is not intended to limit the authority of the FTC or other executive agencies, FCC regulation of common carriers as to information security breaches or any other Federal law (unless the APRA so states) or to "modify, impair, supersede the operation of, or preclude the application" of antitrust laws (Section 20(b)(2)). Further, the APRA draft does not exempt compliance obligations imposed by the Children's Online Privacy Protection Act of 1998, which also is enforceable by state attorneys general. (Section 21).

How does the APRA draft handle enforcement?

State Enforcement

Section 18 of the APRA draft authorizes enforcement by state attorneys general, chief consumer protection officers, and any other "officer" of "officer of a State" (e.g., an agency empowered to

enforce privacy laws like the **California Privacy Protection Agency** under CCPA) in Federal district court. These authorized state-level APRA enforcers may seek injunctive relief; civil penalties, damages, restitution and other consumer compensation; attorneys' fees and other litigation costs; and other relief, as appropriate. The state-level APRA enforcers must notify the FTC prior to initiating a civil action "except where not feasible" and otherwise immediately after initiating the civil action.

FTC Enforcement

Section 17 also provides for FTC enforcement. The APRA draft does not exempt "common carriers subject to title II of the Communications Act of 1934" or non-profit organizations (n.b., the state consumer privacy laws of New Jersey, Colorado and Oregon also apply to federally exempt nonprofit organizations). Accordingly, these two types of entities are subject to FTC enforcement via the APRA draft. (Section 17(b)(3)). These types of entities typically are not subject to FTC enforcement under Section 5 of the FTC Act. If the FTC has initiated an action against a defendant, states are prohibited from initiating their own action based on any APRA violation alleged in the FTC's complaint. Presumably, the FTC and the authorized state officers could still participate in powerful multistate investigations involving privacy violations and consumer protection claims. The FTC is permitted in some areas and required in others to issue regulations under the APRA, including for privacy impact assessments, universal opt-out mechanisms, processed-based data security, exceptions "to protect the rights of individuals," exceptions to "alleviate undue burdens on covered entities," and exceptions to "prevent unjust or unreasonable outcomes from the exercise of" the APRA draft's access, correction, deletion, and portability rights. The FTC also is directed to establish, within a year after enactment, a new privacy bureau that is comparable to the FTC's existing consumer protection and competition bureaus. The APRA draft provides for a 180-day cure period for alleged violations of Sections 15 and 16.

The draft APRA gives the FTC more teeth than it has under Section 5 absent rulemaking. A violation of the APRA draft is "a violation of a rule defining an unfair or deceptive act or practice" (Section 17(b)(1)) and therefore subject to $51,744 (adjusted annually for inflation) in civil penalties per violation under Section 5(m)(1)(A) of the FTC Act, and the FTC may commence a civil action for consumer redress (e.g., disgorgement) under Section 19 of the FTC Act.

Private Right of Action

Section 19 of the APRA draft allows for a limited private right of action (PRA) related to violations of specific APRA provisions, including transfers of sensitive covered data.

This PRA allows for recovery of actual damages, injunctive relief, declaratory relief, and reasonable attorneys' fees and costs for violations of most of the APRA's provisions. Statutory damages are allowed only in limited circumstances, consistent with the Illinois Biometric Privacy Act (BIPA) and a violation of the California Consumer Privacy Act that result in a data breach.

Thirty (30) days prior to initiating an action, unless a "substantial privacy harm" is alleged, the individual must provide the covered entity with a "written notice identifying the specific provisions of [APRA]" that the individual alleges the covered entity violated. (The APRA draft defines "substantial privacy harm" as an alleged financial harm of $10,000 or more or an alleged physical or mental harm to an individual that involves treatment by a licensed health care provider, physical injury, highly offensive intrusion into an individual's reasonable expectation of privacy or discrimination on the basis of race, color, religion, national origin, sex, or disability.) The APRA draft also provides for a 30-day cure period to qualify for injunctive relief, excepting for substantial privacy harms.

A pre-dispute arbitration agreement is not valid or enforceable "at the election of the individual alleging [an APRA violation]" for an individual under age 18 or if the alleged violation resulted in a substantial privacy harm."

While quantifying actual damages may prove difficult in some cases, the ability to seek injunctive and declaratory relief and obtain attorney's fees and costs will most certainly foster "private attorney general" actions by the plaintiffs' bar and consumer advocates, a stated intent of one of the co-sponsors. This is likely to trigger the most significant policy debate concerning the APRA draft.

Based on the APRA draft, when would APRA go into effect?

The APRA would be effective 180 days after enactment (Section 24).

As noted above, the FTC is permitted (in some sections) or required (such as for opt-in mechanism) to issue regulations, which may include varying enforcement timelines and new or different obligations.

Has Congress considered other comprehensive privacy legislation in recent years?

Yes. A comprehensive national data privacy and security bill titled the *American Data Privacy and Protection Act* (ADPPA) was considered in 2022, during the 117th Congress.

A group of three prominent lawmakers – Rep. Rodgers, Rep. Frank Pallone (D-NJ) and Sen. Roger Wicker (R-MS) – appeared to have momentum with compromises on two key issues: (1) federal pre-emption of state laws, and (2) a private right of action (i.e., an individual's right to file for ADPPA violations). The ADPPA advanced out of the House Committee on Energy and Commerce But, then-Speaker of the House Nancy Pelosi (D-CA) – who controlled the House floor legislative agenda – and other California delegation lawmakers were reportedly concerned about federal pre-emption because ADPPA did not provide the same protections as California's landmark privacy law, California Consumer Privacy Act (CCPA). In the Senate, Sen. Cantwell also criticized the ADPPA for "**major enforcement holes**." Momentum stalled on the ADPPA and the 117th Congress adjourned, sending ADPPA to that congress' legislative graveyard.

Will the APRA draft become law this year?

The APRA draft is just that: a draft that is up for discussion and has yet to be introduced formally. Congressional staff has indicated Chairs Rodgers and Cantwell will introduce their bills shortly, and APRA will move through regular legislative order. The House's APRA draft is now scheduled to be discussed at a subcommittee hearing next week. If this process proceeds as intended, the language will be discussed during committee hearings, likely amended during committee mark-ups and debated on the floor in each chamber before the full House and Senate each vote. If the House-passed and Senate-passed versions of the bill differ, contrasts will need to be ironed out before identical, compromise legislation is passed in each chamber and forwarded to the president's desk for signature.

There are motivations on both sides of the aisle to get a privacy bill across the finish line by the end of the year. Chair Rodgers is retiring and may view APRA as a 'legacy bill'; other lawmakers may consider the prospects of different majorities in the House and Senate next year or a different president in the White House. Additionally, with the emergence of artificial intelligence (AI) into the policy spotlight, many Democratic and Republican lawmakers quickly realized that the lack of a federal data privacy law was likely hindering their ability to address some AI concerns (Chair Rodgers has repeatedly emphasized the need for a national data privacy standard as a "first step towards a safe and prosperous AI future.") Furthermore, many Democrats, who believe they have benefited at the ballot box for speaking out against the Supreme Court's abortion decision in *Dobbs v. Jackson Women's Health Organization*, are eager to pass a federal privacy law that addresses issues they say are now raised by consumer health apps and other health and tracking technologies.

With only nine months left of the 118th Congress, some observers may question whether lawmakers can pass comprehensive privacy legislation this year. A "regular order" process can take

time. Over the past week, additional committee chairs in the House have asserted jurisdictional claims to data privacy topics; hearings and markups in multiple committees could lengthen the legislative timeline even further. Chair Rodgers aspires for a House vote by May 24, but the 2024 congressional calendar is tight. There are deadline-driven reauthorizations and appropriations to be considered that take up valuable floor time, as well as upcoming recesses that allow lawmakers to leave Washington for work and/or campaigning in their home states and districts.

Consensus is needed to get a bill enacted into law, especially in the 118th Congress, where majorities in the House and Senate are particularly narrow. While Chair Rodgers has indicated she is "**having conversations with both House and Senate leadership right now**," questions remain on how much support APRA could garner. To advance to a final vote in the Senate, sixty votes are generally needed. In the House, due to some Republicans blocking legislative votes by rejecting measures to tee up floor debates, House Speaker Mike Johnson (R-LA) has been bringing legislation to the full chamber under suspension of the rules. "Suspension of the rules" allows House Members to vote on measures with broad support in an expedited manner. Debate time is shortened to 40 minutes, but the threshold for passage is increased, to two-thirds of Members voting for or against, instead of a simple majority.

For their parts, Chair Rodgers' and Chair Cantwell's committee counterparts have expressed a willingness to review the legislation, but have already raised concerns. House Committee on Energy and Commerce Ranking Member Pallone referred to the discussion draft as "very strong" and "built on the foundation of years of hard work." However, he also said "[t]here are some key areas where I think we can strengthen the bill, especially in children's privacy." Senate Committee on Commerce, Science and Transportation Ranking Member Ted Cruz (R-TX) stated he would not "support any data privacy bill that empowers trial lawyers, strengthens Big Tech by imposing crushing new regulatory costs on upstart competitors or gives unprecedented power to the FTC to become referees of internet speech and DEI compliance."

Some lawmakers may push back against APRA's pre-emption of state requirements, especially those from California, as happened during efforts to pass the ADPPA. California was the first state to pass a data privacy law in 2018, with 14 states since following suit (Some of these state data privacy laws are set to take effect in 2025). Not surprisingly, on April 8, California's top privacy enforcer came out in opposition of the APRA draft. California Privacy Protection Agency Executive Director Ashkan Soltani told MLex: "Americans shouldn't have to settle for a federal privacy law that limits states' ability to advance strong protections in response to rapid changes in technology and emerging threats in policy – particularly when Californians' fundamental rights are at stake. Congress should set a floor, not a ceiling."

In highly politicized Washington, it remains uncertain whether APRA will be eclipsed by the start of the 119th Congress in January 2025, or if current lawmakers will be able to get legislation across the finish line this year, including during a potential "lame duck" session after the November congressional and presidential elections. To be sure, even if an APRA bill does not pass this year, it will serve as the new template for future privacy legislative debates and will help shape ongoing federal AI legislative efforts.

Privacy World will continue to cover updates related to privacy law developments in the U.S. and around the world. Please contact the authors for more information.

Disclaimer: While every effort has been made to ensure that the information contained in this article is accurate, neither its authors nor Squire Patton Boggs accepts responsibility for any errors or omissions. The content of this article is for general information only, and is not intended to constitute or be relied upon as legal advice.

---

[1] This analysis is based on the version released by Chair Cantwell on April 7, 2024. The House Committee on Energy and Commerce released an updated House **draft** on April 9, 2024, in advance of next week's legislative hearing. However, the differences are not material and mostly grammatical or organizational.
