THORN RUN PARTNERS
GOVERNMENT RELATIONS

Memorandum

April 12, 2024

THE AMERICAN PRIVACY RIGHTS ACT: BREAKDOWN AND SIDE-BY-SIDE ANALYSIS

INTRODUCTION

On April 8, House Energy and Commerce (E&C) Committee Chair Cathy McMorris Rodgers (R-WA) and Senate Commerce Committee Chair Maria Cantwell (D-WA) announced the bipartisan, bicameral American Privacy Rights Act (APRA) of 2024 (discussion draft; section-by-section). The APRA would establish a comprehensive framework for a national data privacy standard to protect consumer data privacy and security, creating new requirements for covered entities with regards to handling data and ensuring consumer rights.

- **Background** — In the 117th Congress, Rep. McMorris Rodgers worked with E&C Ranking Member Frank Pallone (D-NJ) and then Senate Commerce Ranking Member Roger Wicker (R-MS) to introduce another major bipartisan, bicameral bill called the American Data Privacy Protection Act (ADPPA) (H.R.8152), which has not been reintroduced this session. However, the ADPPA ultimately failed to gain traction for a few reasons: first, Speaker Nancy Pelosi (D-CA) refused to bring the ADPPA up for a floor vote due to concerns that it would undermine California's own data privacy law; and second, Sen. Cantwell opposed the ADPPA because she believed that its private right of action was not sufficiently robust.

Now that the California delegation, without Speaker Pelosi, has less sway over the House and is apparently — according to legislative aides for Rep. McMorris Rodgers and Sen. Cantwell — placated by the strengthened private right of action in the APRA, this new data privacy agreement may have a path forward this Congress. However, there are some other factors at play:

- **Opposition** —Compared to the ADPPA, the APRA provides for a somewhat broader private right of action, alongside jettisoning the four-year delay that was outlined in the ADPPA. Republicans have long raised concerns about the potential costs of an expansive private right of action since it opens up covered entities to significant litigation risk. However, the APRA still maintains significant limitations on private right of action, meaning it may not necessarily be a sticking point for all Republican lawmakers.

- **Election year politics** — With the 2024 election cycle in full swing, it is possible that concerns from Republicans about handing the Biden administration a "win" to campaign on will delay passage of the APRA in the coming months. However, during the post-election "lame duck," there may be an opportunity for Congress to pass the APRA, alongside a number of other legislative priorities. Proponents of the legislation are likely to make a concerted effort to pass the legislation before the end of the calendar year, especially considering the coming retirement of Rep. McMorris Rodgers.

- **Lobbying blitz** — Introduction of the APRA will be accompanied by a flurry of lobbying activity as big tech companies seek to voice their concerns about the legislation. Similarly, consumer advocacy groups, state governments, and other stakeholders will ramp up their advocacy efforts on Capitol Hill, either emphasizing their support for or opposition to the legislative framework.

- **Kids online protections** — Compared to the ADPPA, the APRA does not have special provisions providing for kids' online protections and privacy. Perhaps proponents of the APRA plan to build support in the upper chamber by having the bill serve as a vehicle for legislation that seeks to establish more online protections for children. A likely candidate is the Kids Online Safety Act (KOSA), with was updated recently and officially sponsored by Senate Majority Leader Chuck Schumer (D-NY). Notably, Sen. Cantwell worked with bill leaders Sens. Marsha Blackburn (R-TN) and Richard Blumental (D-CT) in order to alleviate concerns that the bill could be used by attorneys general in red states to limit LGBTQ+ content on social media platforms.

Looking ahead — Rep. McMorris Rodgers and Sen. Cantwell will likely push for expedient consideration and passage of the APRA in the coming weeks and months. It is important to note that both Rep. McMorris Rodgers and Sen. Cantwell have emphasized that the APRA discussion draft is likely to be altered in the near future as feedback is gathered from lawmakers and stakeholders. On April 17, the House E&C Subcommittee on Innovation, Data, and Commerce will hold a hearing to discuss the APRA, among other data privacy and online safety measures. This hearing will likely be followed by subcommittee markup, full committee markup, and then House consideration under suspension of the rules assuming the APRA has bipartisan support. Senate Commerce will also likely try to markup the APRA. However, Ranking Member Ted Cruz (R-TX) has already expressed concerns regarding the legislation, in particular around the expansion of Federal Trade Commission (FTC) authority. There are also competing must-pass legislative issues that will take up bandwidth in both chambers, including Federal Aviation Administration (FAA) reauthorization.

TABLE OF CONTENTS

BREAKDOWN

Key Definitions			
	APRA	**ADPPA**	**Takeaways**
Covered Entity	• Any entity that determines the purpose and means of collecting, processing, retaining, or transferring covered data and is subject to the FTC Act, including common carriers and certain nonprofits. • Small businesses, governments, entities working on behalf of governments, the National Center for Missing and Exploited Children (NCMEC), and, except for data security obligations, fraud-fighting non-profits are excluded.	• Any entity that collects, processes, or transfers covered data and is subject to the jurisdiction of the FTC, including nonprofits, and telecommunications common carriers. • Exceptions are provided for small and medium-sized covered entities.	• No substantial differences
Covered Data	• Information that identifies or is linked or reasonably linkable to an individual or device. • Does not include de-identified data, employee data, publicly available information, inferences made from multiple sources of publicly available information that do not meet the definition of sensitive covered data and are not combined with covered data, and information	• Information identifying, linked, or reasonably linkable to an individual or device linkable to an individual. This includes derived data and unique identifiers. • Does not include de-identified data, employee data, or publicly available information.	• No substantial differences.

	in a library, archive, or museum collection subject to specific limitations.		
Sensitive Covered Data	• A subset of covered data that includes numerous specific categories, including government identifiers, health information, biometric information, financial account and payment data, precise geolocation information, and many more. • Any information related to individuals under 17 is sensitive.		
Covered Algorithms	• A computational process — including one derived from machine learning, statistics, or other data processing or artificial intelligence (AI) techniques — that makes a decision or facilitates human decision-making by using covered data, which includes determining the provision of products or services or ranking, ordering, promoting, recommending, amplifying, or similarly determining the delivery or display of information to an individual.		
Large Data Holder	• Covered entities that have $250 million or more in annual revenue; collect, process, retain, or transfer the covered data of more than five million individuals (or 15 million portable devices or 35 million connected devices that are linkable to an individual) or the sensitive data of more than 200,000 individuals (or 300,000 portable devices or 700,000 connected devices).	• Covered entities with gross revenues above $250 million; collect, process, or transfer covered data of over five million individuals/devices or the sensitive covered data of 100,000 individuals/devices.	• The ADPPA's definition of large data holder is slightly narrower than the APRA.
Data Brokers or Third-Party Collecting Entities	• Any covered entity whose principal source of revenue is derived from processing or transferring covered data that the covered entity did not collect directly from the individuals linked or linkable to such covered data.	• Any covered entity whose principal source of revenue is derived from processing or transferring covered data that the covered entity did not collect directly from the individuals linked or linkable to the covered data.	• While the APRA refers to such entities as "data brokers," the definition remains largely unchanged from the ADPPA's "third-party collecting entities."

	• Does not include an entity to the extent that such an entity is acting as a service provider.	• Does not include a covered entity insofar as such entity processes employee data collected by and received from a third party concerning any individual who is an employee of the third party for the sole purpose of such third party providing benefits to the employee.	
Targeted Advertising	• Displaying an online advertisement based on known or predicted preferences or interests associated with an individual or device identified by a unique identifier. • Does not include advertisements in response to an individual's specific request for information; first-party advertising; contextual advertising; or processing data for measurement.	• Presenting to an individual or device identified by a unique identifier, or groups of individuals or devices identified by unique identifiers, an online advertisement that is selected based on known or predicted preferences, characteristics, or interests associated with the individual or a device identified by a unique identifier. • Does not include advertising or marketing to an individual or an individual's device in response to the individual's specific request for information or feedback; contextual advertising; or processing data for measurement.	• No substantial differences.
Small Business	• Businesses that have $40 million or less in annual revenue; collect, process, retain, or transfer the covered data of 200,000 or fewer individuals (not including credit	• Covered entities or service providers with annual gross revenues that do not exceed $41 million; collect or process the covered data of fewer than 200,000	• The APRA provides a revised small business definition to remove a percentage of revenue nexus to data exchanges.

	card swipe and other transient data); and do not earn revenue from the transfer of covered data to third parties.	individuals; and do not derive more than 50 percent of their revenue from transferring covered data.	

Key Provisions			
	APRA	**ADPPA**	**Takeaways**
Effective Date	• Both measures would take effect 180 days after enactment.		
Private Right of Action	• Immediately after the APRA goes into effect, consumers would be allowed to file private lawsuits against entities that violate the law. • An action for a substantial privacy harm or by a minor could not be subject to mandatory arbitration. • Entities would be provided an opportunity to cure in actions requesting injunctive relief and written notice in actions seeking actual damages, except for actions for a substantial privacy harm.	• Starting two years after the ADPPA takes effect, persons or classes of persons would generally be permitted to bring a civil action in federal court seeking compensatory damages, injunctive relief, declaratory relief, and reasonable litigation costs. • Covered entities could not enforce pre-dispute arbitration agreements or joint action waivers with respect to minors. • When individuals seek injunctive relief against covered entities or any relief against small- and medium-sized entities, those entities would have a limited right to cure the alleged deficiency.	• One of the most significant differences between the ADPPA and APRA pertains to private right of action. • The ADPPA would allow individuals to bring civil actions seeking compensatory or injunctive relief against **covered entities starting four years after the law went into effect**, though there were rumors that this had been decreased to two years throughout the course of negotiations. **Individuals would have to first notify their state attorney general and the FTC of their intent to bring a suit** and, to limit redundant actions, individuals could not file their own lawsuit if the state or FTC had already filed one. If a covered entity successfully **cures an alleged problem within 45 days**, they could

			seek dismissal of a demand for injunctive relief. • Private right of action in the APRA is somewhat broader. Significantly, unlike the ADPPA, the **APRA omits language that would have delayed the private right of actions for four years after enactment.** The legislation also **omits language requiring individuals to first notify their state attorney general and the FTC** of their intent to bring a suit. The draft bill would also **render pre-dispute arbitration agreements unenforceable** for claims involving minors or alleging "substantial privacy harms," defined as those involving financial harms of at least $10,000, mental or physical injury, or discrimination based on protected classes. Under the APRA, companies would have **30 days to cure a harm** before a plaintiff could pursue litigation.
Federal and State Enforcement	• The APRA would provide for enforcement by the FTC, which would be directed to establish a new bureau to carry out its authority under the law. • State attorneys general, chief consumer protection officers,	• Similarly, the ADPPA would provide for enforcement by the FTC, which would be directed to establish a new bureau to carry out its authority under the law. • State attorneys general and chief consumer protection enforcement	• Both bills would give the **FTC, state attorneys general, and chief state consumer protection enforcement officers** the ability to take enforcement actions. • However, unlike the ADPPA, the **APRA would also authorize other officers**

	and other officers of a state would be authorized to take enforcement actions.	officers would also be allowed to bring cases in federal court.	**of the state** to take enforcement actions. • Under both measures, **telecommunications "common carriers"** as defined by the Communications Act of 1934 would be defined as covered entities and, for the purposes of the requirements under the bills, fall under the jurisdiction of the FTC.
Preemption	• State laws covered by the APRA would be preempted, with the exception of an enumerated list of state laws, such as consumer protection laws, civil rights laws, criminal laws unrelated to data privacy, etc. • Entities subject to and in compliance with other specified federal privacy laws — including the Gramm-Leach-Bliley Act (GLBA) and HIPAA — would be deemed in compliance with the related provisions or the APRA other than data security.	• State laws covered by the ADPPA would be similarly preempted, except for an enumerated list of state laws. • Covered entities subject to and in compliance with the related data privacy and security requirements of certain specified federal laws would be held to be in compliance with the related laws of the ADPPA solely and exclusively to the extent that covered data is subject to the requirements in the other laws.	• While both the APRA and ADPPA generally aimed to preempt state laws, the APRA alters several provisions to **alleviate concerns that the ADPPA might not have sufficiently preempted state laws**. For instance, the APRA provides for preemption with an additional "purpose" section that states the bill is to "establish a uniform national data privacy and data security standard in the United States." • Ultimately, both measures provide for a series of excepted laws and topics where they would not preempt state and federal sectoral laws.
HIPAA and Non-HIPAA Health Information	• Both the APRA and the ADPPA contain a carve-out for HIPAA, meaning the requirements established by the bills do not apply to types of data and entities regulated under HIPAA. **The carve-out presumably includes personal information collected in the context of HIPAA subject data or research activity,** such as clinical trials. • However, it is important to note that the **APRA and ADPPA would in fact apply to health data that is collected by, transferred to, or retained by non-HIPAA covered entities**. Specifically, the APRA defines this type of non-HIPAA health information as "information that describes or reveals the past, present, or future physical health, mental health,		

	disability, diagnosis, or health condition or treatment of an individual, including the precise geolocation information of such treatment." The ADPPA's definition is not substantially different.		
Data Protections for Children and Minors	• The APRA would treat information about "covered minors" — which is defined as individuals under the age of 17 — as sensitive covered data.	• Covered entities would be subject to additional requirements for covered data with respect to individuals under age 17. Targeted advertising would be expressly prohibited if covered entities have actual knowledge that an individual is under 17. Where the covered entity has actual knowledge the individual is between 13 and 17, covered entities could not transfer the covered data of individuals between 13 and 17 years old to third parties without express affirmative consent.	• The **ADPPA has special provisions related to kids and teens under 17**, such as a prohibition on all targeted advertising to such minors and strict limits on the ability to transfer minors' data to third parties. The ADPPA would also establish a Youth Privacy and Marketing Division at the FTC that would be dedicated to children's privacy. • Although the APRA also contains child-specific provisions — such as treating minors' data as "sensitive covered data" — **it does not contain many of the ADPPA's minor-specific provisions** and would not create a new division at the FTC.
Civil Rights and Algorithms	• Collecting, processing, retaining, or transferring covered data in a manner that discriminates on the basis of race, color, religion, national origin, sex, or disability would be prohibited. • Large data holders that use covered algorithms in a manner that pose a "consequential risk" of harm must conduct an impact assessment and must provide	• Covered entities would not be allowed to collect, process, or transfer covered data in a manner that discriminates on the basis of race, color, religion, national origin, gender, sexual orientation, or disability. • Large data holders that use algorithms would be required to assess their algorithms annually and submit these impact assessments to the FTC.	• Both bills would **explicitly extend legal protections for protected classes** to algorithms and related activities. • While the APRA would also require algorithmic impact assessments, it differs from the ADPPA as it **seeks to address concerns about the broadness of assessments** by specifically delineating categories for when they must be conducted.

	the assessment to the FTC and make it publicly available. • Specifically, impact assessments must be conducted when they pose a consequential risk pertaining to: (1) covered minors; (2) housing, education, employment, health care, insurance, or credit opportunities; (3) public accommodations; (4) disparate impacts based on race, color, religion, and sex; and (5) disparate impact based on political party registration.		
Data Minimization	• Covered entities and service providers would not be able to collect, process, retain, or transfer data beyond what is necessary, proportionate, or limited to provide or maintain a product or service requested by an individual, or provide a communication reasonably anticipated in the context of the relationship, or a permitted purpose. • Permitted purposes include protecting data security; complying with legal obligations; effectuating a product recall or	• The ADPPA would impose a baseline duty on all covered entities not to unnecessarily collect or use covered data in the first instance, regardless of any consent or transparency requirements. Specifically, covered entities would be prohibited from collecting, processing, or transferring covered data beyond what is reasonably necessary, proportionate, and limited to provide specific products and services requested by individuals, communicate with individuals in a manner they reasonably anticipate given the	• **Both bills would establish data minimization requirements**, which require organizations to collect, retain, and transfer no more data than is necessary to meet specific needs. • **There are exceptions**, however, and each bill enumerates a series of "permitted" or "permissible" purposes. The APRA revises some of these categories, including a broader carveout for criminal activity.

	fulfilling a warranty; conducting market research; de-identifying data for use in product improvement and research, among many others.	context of their relationship with the covered entity, or for a purpose expressly permissible by the bill. • Permissible purposes also include protecting data security; complying with legal obligations; effectuating a product recall or fulfilling a warranty; conducting market research; de-identifying data for use in product improvement and research, among many others.	
Transparency	• Covered entities and service providers would be required to have publicly available privacy policies detailing their data privacy and security purposes. • The privacy policies must identify the entity; disclose the categories of data collected, processed, or retained; the purposes for the data processing; the categories of service providers and third parties to which data is transferred; the name of any data brokers to which data is transferred; the length of time data is retained; data security practices; and the effective date of the privacy policy.	• Covered entities would be required to provide individuals with privacy policies detailing their collection, processing, transfer, and security activities in an understandable manner. • Such policies must include contact information, the affiliates of the covered entity that it transfers covered data to, and the purposes for each category of covered data the covered entity collects, processes, and transfers. Covered entities must specify the third-party collecting entities to whom they transfer covered data and for what purposes.	• No substantial differences.

Consumer Rights	• Consumers would be given the right to access their covered data and to know the name of any third party or service provider to which the data was transferred and the purpose of the transfer. • Upon a verified request, covered entities would also be required to: (1) correct inaccurate or incomplete covered data; (2) delete covered data; and (3) export covered data.	• Consumers would similarly be given the right to access, correct, delete, and portability of, covered data that pertains to them. • The right to access includes obtaining covered data in a human-readable and downloaded format, the names of any other entities their data was transferred to, and the purposes for transferring the data.	• No substantial differences — both the APRA and ADPPA would give consumers the right to access, port, rectify, and delete their personal data.
Opt-Out & Targeted Advertising	• Consumers would be given the right to opt out of the transfer of non-sensitive covered data. • A covered entity would not be able to transfer sensitive covered data to a third party without the affirmative express consent of the individual to whom such data pertains. • The FTC would be directed to issue regulations to establish the requirements and technical specifications for a centralized mechanism for individuals to exercise the opt-out rights. • Consumers would also be allowed to opt out of the use of their personal information for targeted advertising.	• Individuals may opt out of the transfer of any covered data to a third party. • Sensitive covered data may not be collected, processed, or transferred to a third party without the express affirmative consent of the individual to whom it pertains. • The FTC would be required to conduct a feasibility study regarding a centralized opt-out mechanism. If the agency concludes that it is feasible, then the FTC would be required to establish such a mechanism. • Covered entities engaged in targeted advertising must provide individuals with clear and conspicuous means to opt out prior	• Both bills require affirmative or opt-in consent for the **collection and transfer of sensitive data** — including biometric and genetic information, in the APRA, and teenagers' data, in the ADPPA — and allow consumers to opt out of the collection and transfer of non-sensitive data. • Additionally, the APRA and ADPPA both instruct the FTC to establish a **centralized opt-out mechanism** that would allow individuals to opt out of all covered data transfers. • Finally, both bills would give consumers the ability to opt-out of the use of their personal information for **targeted advertising**.

		to any targeted advertising and at all times afterwards.	
Dark Patterns	• The bill would prohibit covered entities from using "dark patterns" to divert an individual's attention from notice, impair the exercise of the aforementioned rights, or obtain consent.	• The ADPPA would prohibit covered entities from attempting to obtain the affirmative express consent of an individual or condition the exercise of a right through the design, modification, or manipulation of any user interface with the purpose of obscuring, subverting, or impairing their decision making.	• In contrast to the APRA, the ADPPA does not make use of the specific term "dark patterns." However, **the bills would both likely have the same effect** in prohibiting the use of dark patterns to impair users' ability to exercise the rights established in the bills.
Data Security	• Under both the APRA and ADPPA, covered entities and service providers would have to establish data security practices that are appropriate to the entity's size, the nature and scope of the data practices, the volume and sensitivity of the data, and the state of the art in safeguards.		
Executive Responsibility	• All covered entities would be required to designate one or more covered employees to serve as privacy or data security officers. • Large data holders would be required to designate both a privacy and a data security officer. • Large data holders would also be directed to file with the FTC annual certifications of internal controls designed to comply with the bills and internal reporting structures for compliance with both measures. • Large data holders must conduct regular privacy impact assessments.		
Service Providers and Third Parties	• Service providers would be required adhere to the instructions of a covered entity and assist the entity in fulfilling its obligations under the APRA. • Service providers would be mandated to cease data practices where they have actual knowledge that a covered entity is in violation of the bill.	• Service providers may only collect or process covered data for the purposes directed by the covered entity it got the data from and may not transfer such data to another entity without express affirmative consent of the individual to whom it pertains. Service providers generally have the same responsibilities as other covered	• No substantial differences.

	• Service providers would have to maintain the security and confidentiality of covered data and allow for independent assessors to assess their security practices. • Covered entities must exercise due diligence in the selection of service providers and in deciding to transfer covered data to a third party, and the FTC is directed to issue guidance regarding compliance with the due diligence requirements. • Third parties may only process, retain, and transfer data received from another entity for a purpose consistent with what the covered entity disclosed in its privacy policy; or, for sensitive covered data, a purpose for which the consumer provided affirmative express consent.	entities, with the exception that, given their non-consumer facing role, they are only required to assist the covered entities they process covered data for from fulfilling requests by individuals to exercise their rights under the ADPPA. • Third parties would be prohibited from processing covered data beyond the expectations of a reasonable individual. • Covered entities must conduct reasonable due diligence in selecting service providers and deciding to transfer covered data to third parties. The FTC would be directed to issue guidance to help covered entities comply with this section, including to help alleviate potentially unreasonable compliance burdens on small entities.	
Data Brokers or Third-Party Collecting Entities	• Under APRA, data brokers would be required to maintain a public website that identifies the entity as a data broker; includes a tool for individuals to exercise their individual controls and opt-out rights; and includes a link to the	• The ADPPA would require third-party collecting entities to place a clear and conspicuous notice on their web site and/or mobile application informing individuals they are a third-party collecting entity using language specified by	• Called "third-party collecting entities" under the ADPPA, the APRA refers such entities as "data brokers." While the thresholds for being counted as one remain the same and the registry continues, **there are new**

	FTC's data broker registry website. The website must be reasonably accessible for individuals with disabilities. • Data brokers would be prohibited from advertising data for the purpose of stalking or fraudulent purposes and are prohibited from misrepresenting their business practices. • The FTC would be directed to establish a data broker registry, and data brokers affecting the data of 5,000 or more individuals must register each calendar year. The registry must include a "do not collect" mechanism for consumers to use. The FTC would also issue guidance regarding the content of a data broker's website.	FTC regulations. The FTC would be required to promulgate regulations under the APA that require third-party collecting entities to allow for auditing of any access to or disclosure of covered data related to individuals that is processed by the third-party collecting entity. • Third-party collecting entities that process covered data of more than 5,000 individuals would be required to annually register with the FTC. Registration includes paying a $100 fee, providing information about the third-party collecting entity's activities, providing contact information, and creating a link to a website where individuals may exercise their audit rights under this section. Third-party collecting entities would face civil fines for failing to register or provide the notice. • Finally, the FTC would be directed to establish and maintain an online, public, searchable registry of registered third-party collecting entities that allows individuals to look up information on third-party collecting entities, links to and contact information of the third-	**requirements such as prohibited practices**.

		party collecting entities, and a link and mechanism by which individuals may submit a single request to all registered third-party collecting entities to have all covered data about them deleted within 30 days.	
Privacy-Enhancing Audits Pilot Program	• The APRA would establish a pilot program at the FTC for entities to deploy privacy-enhancing technologies. • Entities can petition to be accepted with a specific privacy-enhancing technology that meets or exceeds the data security requirements of this Act. • Participation in the pilot program entitles a covered entity to a rebuttable presumption of compliance with the data security requirements of this Act for a private right of action related to a data breach.	**N/A**	• The APRA would establish a new pilot program meant to incentive the deployment of **privacy-enhancing technologies**.
Retaliation	• Covered entities may not retaliate against individuals for exercising their rights under both measures, including by denying or charging different rates for goods or services.		