

# Client Alert

Data, Privacy and Security

**MAY 13, 2024**

For more information,  
contact:

Emily R. Apte  
+1 512 457 2011  
[eapte@kslaw.com](mailto:eapte@kslaw.com)

Jesse Snyder  
+1 202 383 8925  
[jsnyder@kslaw.com](mailto:jsnyder@kslaw.com)

Katrina Jackson  
+1 202 626 2640  
[kjackson@kslaw.com](mailto:kjackson@kslaw.com)

Jillion Simons  
+1 404 572 2721  
[jsimons@kslaw.com](mailto:jsimons@kslaw.com)

---

## King & Spalding

Austin  
500 West 2nd Street  
Suite 1800  
Austin, Texas 78701  
Tel. +1 512 457 2000

Washington, D.C.  
1700 Pennsylvania Avenue,  
NW  
Suite 900  
Washington, D.C. 20006  
Tel. +1 202 737 0500

## American Privacy Rights Act of 2024 Insights

In April, 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) introduced the American Privacy Rights Act of 2024 (APRA), a bicameral and bipartisan federal comprehensive privacy bill that would provide multiple governmental enforcement mechanisms, including for the Federal Trade Commission (FTC) and state attorneys general, as well as a private right of action for certain breaches of defined privacy rights. The draft APRA expands upon the American Data Privacy Protection Act (ADPPA), which was considered last Congress in 2022.

As drafted, the APRA has sweeping coverage and would apply to entities that (1) determine the purpose and means of collecting, processing, retaining, or transferring covered data; and that (2) are subject to the FTC's authority under the FTC Act, including common carriers and certain nonprofits. See American Privacy Rights Act of 2024, Sec. 2 (10)(A)(i). The bill also outlines various requirements for large data holders, data brokers, and covered high-impact social-media companies. *Id.* at Sec. 2 (25)(13)(11). The APRA's tiered approach would instantiate sweeping coverage, all while including exemptions for small businesses, governments, as well as entities that are "collecting, processing, retaining, or transferring covered data" on behalf of a government entity, and fraud-fighting non-profits. *Id.* at Sec. 2 (10).

The APRA focuses on two types of consumer data: "covered data" and "sensitive covered data." Covered data includes "information that identifies or is linked or reasonably linkable to an individual or device," *Id.* at Sec. 2 (9)(A), but does not include de-identified data, employee data, or publicly available information. *Id.* at Sec. 2 (9)(B). "Sensitive covered data" is a subset of covered data and would embrace an extensive list of data elements including: government identifiers; health, genetic, and biometric information; financial account and payment data; precise geolocation information; and login credentials. *Id.* at Sec. 2 (34). But



other data elements that are relatively novel—private communications; online activities over time and across third-party websites and high-impact social media sites; and calendar or address book data, phone logs, photos and recordings for private use—in addition to any other data the FTC defines as sensitive covered data by rule. *Id.* at Sec. 2 (34). This catch-all attempts to future proof the definitions by allowing the FTC to incorporate additional data elements via its rulemaking process in lieu of amending the legislation.

The APRA incorporates the concept of data minimization by focusing on consumer transparency alongside appropriate consent processes and mechanisms. For example, the drafted legislation requires covered entities to obtain consumers’ “affirmative express consent” to (1) collect or transfer to a third party the consumers’ biometric or genetic information, (2) transfer consumers’ sensitive data to a third party, and (3) allow consumer participation in a bona fide loyalty program and for the transfer of any covered data collected under a bona fide loyalty program. *Id.* at Sec. 3 (c)(1), Sec. 3(c)(2)-(3), & Sec. 8 (b)(1)(i)(I). The APRA also sets out several requirements for obtaining sufficient consent under the definition of “affirmative express consent.” Those requirements include (among other things) that the disclosure be clear and conspicuous, written in easy-to-understand language, meet accessibility standards, and include a prominent heading. *Id.* at Sec. 2 (1)(B).

Similar to some current state privacy laws, moreover, the APRA would establish rights to access covered data, to correct inaccurate or incomplete covered data, to delete covered data, and to export covered data. Most critically, however, the draft legislation would distinctly permit individuals the right to access specific names of any third parties or service providers to whom covered data has been transferred as well as the purpose of behind the transfer.

The APRA acknowledges that there is a growing body of comprehensive state-level privacy laws, and it discusses preemption of these laws in Section 20. In doing so, legislation generally states that no state may “adopt, maintain, enforce, or continue in effect any law, regulation, rule, or requirement” covered by the provisions of or rules relating to the APRA. *Id.* at Sec. 20 (a)(2). Yet there are general exceptions, organized by topic, to include (1) general consumer protection, (2) civil rights, (3) employee and student protections, and (4) data breach notification. *Id.* at Sec. 20 (a)(3). The APRA also allows for specific carveouts as to the California Consumer Privacy Act (CCPA) and the Illinois Biometric Information Privacy Act and its Genetic Information Privacy Act. As for CCPA, where there has been alleged unauthorized access of covered information, the APRA allows for California residents to be awarded the same relief as permitted under the CCPA Section 1798.150. *Id.* at Sec. 19 (a)(2)(C)(i). And for the Illinois laws, the APRA allows for consumers to bring civil actions under such laws when the alleged violation primarily and substantially occurred in Illinois and relate to biometric or genetic information. *Id.* at Sec. 19 (a)(2)(B).

The authors of the APRA, committee Chairs Cathy McMorris Rodgers (R-WA) and Chair Maria Cantwell (D-WA), face a number of challenges in their effort to getting the bill to President Biden’s desk, perhaps the chief one being the relatively few number of legislative days remaining until the presidential election. And beyond timing logistics, Senate Commerce Ranking Member Ted Cruz (R-TX) has expressed his concerns over the drafted APRA, announcing that he “cannot 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.” However, as a bright spot for APRA, on April 17, 2024, the Subcommittee on Innovation Data and Commerce held a hearing titled “Legislative Solutions to Protect Kids Online and Ensure Americans’ Data Privacy Rights,” which was fairly promising for the legislation. Specifically, during the hearing, Subcommittee Chairman Gus Bilirakis (R-FL) asked whether the APRA is the best chance we have at accomplishing comprehensive data privacy, and without hesitation all witnesses answered “yes.” The hearing highlighted the substantial support the APRA has received across both sides of the aisle, however, witnesses expressed disagreement on issues like data broker regulations. While



reports suggests that many are indeed hopeful that the drafted legislation will markedly game change the privacy-and-data-security landscape and obligations for entities that collect and process personal information, disagreement of the details continues to prevail.

The hearing’s witnesses included: Ms. Ava Smithing, Director of Advocacy, Young People’s Alliance, The Honorable Maureen K. Ohlhausen, Co-chair, 21 Century Privacy Coalition, Ms. Katherine Kuehn, Member, Board of Directors and CISO-in-Residence, National Technology Security Coalition, Ms. Kara Frederick, Director, Tech Policy Center, The Heritage Foundation, Mr. Samir C. Jain, Vice President of Policy, Center for Democracy & Technology, and Mr. David Brody, Managing Attorney, Digital Justice Initiative, Lawyers’ Committee for Civil Rights Under Law.

We will continue to monitor the APRA as the dates for the bill to be formally introduced in either Chamber have yet to be set. And while the bill is still in the early phases of the legislation process, companies should attune to possibility of a national standard for compliance.

---

#### ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,300 lawyers in 24 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice.

In some jurisdictions, this may be considered “Attorney Advertising.” View our [Privacy Notice](#).

ABU DHABI	CHARLOTTE	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY
ATLANTA	CHICAGO	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE
AUSTIN	DALLAS	GENEVA	MIAMI	RIYADH	TOKYO
BRUSSELS	DENVER	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.