POLSINELLI. What a law firm should be.™

U.S. Federal Privacy Bill Unveiled

On April 5, 2024 members of U.S. Congress released a draft bipartisan, bicameral federal privacy bill, the **American Privacy Rights Act**. In a **press release**, the stated goal of this legislation is to be "a national data privacy and security standard that gives people the right to control their personal information." As currently drafted, the draft legislation draws from many of the current state comprehensive privacy laws, though there are a number of nuances. We are monitoring the development of this privacy bill and will update as developments arise.

What data is protected under the draft American Privacy Rights Act?

As currently drafted, "covered data" is protected. "Covered data" is information that identifies or is linked or reasonably linkable to an individual or device. Exclusions from the definition of "covered data," include, for example, de-identified data, employee data, publicly available information, and information in a library, archive, or museum collection subject to specific limitations.

Who is subject to the draft American Privacy Rights Act?

As currently drafted, entities that, alone or jointly with others, determine the purposes and means of collecting, processing, or transferring covered data and are subject to the FTC Act, including common carriers and certain non-profits are subject to the law. Service providers to such covered entities are also subject to the law. Currently excluded from the definition of covered entity are government entities (and their service providers), small businesses, and the National Center for Missing and Exploited Children. Certain nonprofits whose primary mission is to prevent, investigate, or deter fraud or to train anti-fraud professionals or educate the public about fraud are generally exempt except for data security obligations. Entities subject to and in compliance with other Federal privacy laws, including the Gramm-Leach-Bliley Act and HIPAA, are deemed to be in compliance with the related privacy provisions of the draft American Privacy Rights Act, though they must still comply with the security provisions of the law.

What does the draft American Privacy Rights Act require?

As currently drafted, the draft legislation draws from many of the current state comprehensive privacy laws. Covered entities and service providers acting on behalf of such covered entities are subject to provisions related to:

- Data minimization: In general, covered entities and service providers are prohibited from (1) processing covered data beyond what is needed 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 (2) processing covered data for a purpose other than those expressly permitted by the draft legislation. Additionally, the draft legislation includes restrictions on the processing of sensitive data and biometric or genetic information.

- Transparency: Similar to other comprehensive privacy laws, the draft American Privacy Rights Act requires covered entities and service providers to have publicly available privacy policies detailing privacy and security practices, including how individuals can exercise their privacy rights.
- Consumer Controls/Rights and Opt-Outs: Similar to other comprehensive privacy laws, the draft American Privacy Rights Act grants individuals the rights of access, correction, deletion, and portability of their covered data. Individuals also have the right to opt out of the transfer (including the disclosure, release, selling, renting, or licensing for consideration of any kind or for a commercial purpose) of their covered data and to opt-out of the use of their covered data for targeted advertising.
- Data Security: Covered entities and services providers are required to establish appropriate data security practices as well as assess vulnerabilities and mitigate reasonably foreseeable risks to consumer data.
- Service Providers: The draft legislation, among other things, requires service provides to enter into contracts with covered entities governing the service provider's data processing on behalf of the covered entity and specifies the content of such contracts.
- Data Brokers: Data brokers, among other things, are required to maintain a public website identifying themselves as a data broker and which includes a tool for individuals to exercise their individual controls and opt-out rights.

Who can enforce the draft American Privacy Rights Act?

The draft legislation provides for both FTC enforcement and enforcement by State attorneys general, chief consumer protection officers, and other officers of a State in Federal district court. In addition, individuals may file private lawsuits against entities that violate their rights. In general, in private lawsuits, courts may award plaintiffs actual damages, injunctive relief, declaratory relief, and reasonable attorney's fees and litigation costs.

Will state comprehensive privacy laws be pre-empted?

Yes. The purpose of the draft legislation is to establish a "uniform national data privacy and data security standard." Under the current draft, state laws covered by the American Privacy Rights Act would be pre-empted, with some exceptions, including, for example, consumer protection laws; civil rights laws; provisions of laws that address the privacy of employees; provisions of laws that address privacy of students; and provisions of laws that address data breach notification.