June 20, 2024 version

The American Privacy Rights Act of 2024

Updated Section-by-Section Summary

This measure would establish national consumer data privacy rights and set standards for data security. The bill also would require covered entities to be transparent about how they use consumer data and give consumers the right to access, correct, delete, and export their data, as well as opt out of targeted advertising and data transfers. The measure would set standards for data minimization that would allow companies to collect and use data only for necessary and limited purposes and prohibit the transfer of sensitive covered data to third parties without the consumer's affirmative express consent. The Federal Trade Commission (FTC), State attorneys general, and consumers could enforce violations of the Act.

DEFINITIONS:

Key definitions include:

- **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.
- **Covered data—**information that identifies or is linked or reasonably linkable to an individual or device. It does not include de-identified data, employee data, publicly available information, on-device data, 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 in a library, archive, or museum collection subject to specific limitations.
- **Publicly available information—**information that has lawfully been made available to the general public. It does not include derived data revealing sensitive covered data, biometric or genetic information, covered data combined with publicly available information, or obscene or non-consensual intimate images.
- **Sensitive covered data—**a subset of covered data that includes government identifiers; health information; biometric information; genetic information; financial account and payment data; precise geolocation information; log-in credentials; private communications; information revealing sexual behavior; calendar or address book data, phone logs, photos and recordings for private use; any medium showing a naked or private area of an individual; video programming viewing information; an individual's race, ethnicity, national origin, religion, or sex, in a manner inconsistent with a reasonable expectation of disclosure; an online activity profile; information about a covered minor; and other data the FTC defines as sensitive covered data by rule.

- **Large data holder—**covered entities that have $250,000,000 or more in annual revenue; collect, process, retain, or transfer the covered data of more than 5,000,000 individuals (or 15,000,000 portable devices or 35,000,000 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).
- **Small business—**businesses that have $40,000,000 or less in annual revenue, adjusted for inflation; collect, process, retain, or transfer the covered data of 200,000 or fewer individuals (not including credit card swipe and other transient data); and do not earn revenue from the transfer of covered data to third parties. Small businesses are exempt from the requirements of the title.
- **Contextual advertising—**presenting or displaying an advertisement that does not vary based on the identity of the individual and is based solely on the content of a webpage or online service, a specific request of the individual for information or feedback, or coarse geolocation data.
- **Direct mail targeted advertising—**advertising or marketing using third-party data through a direct communication with an individual via direct mail.
- **Email targeted advertising—**advertising or marketing using third-party data through a direct communication with an individual via email.
- **First party advertising—**advertising or marketing by a first party using that first party's first-party data and not other forms of covered data though direct communication and entirely within first party context, other than by a high impact social media company for a product not offered by the high-impact social media company.
- **Targeted advertising—**displaying an online advertisement based on predicted preferences or interests associated with the individual or a device identified by a unique persistent identifier. It includes an online advertisement for a product or service by a covered high-impact social media company that is not a product or service offered by the covered high-impact social media company and an online advertisement for a product or service based on the previous interaction of an individual or a device identified by a unique persistent identifier with such product or service on a website or online service that does not share common branding or affiliation with the website or online service displaying or presenting the advertisement.

DATA MINIMIZATION:

- Covered entities and service providers operating on their behalf shall not 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.
- A covered entity cannot collect, process, or transfer to a third party biometric or genetic information without the individual's affirmative express consent. There are strict retention limitations on biometric information.
- A covered entity cannot transfer sensitive data to a third party without the individual's affirmative express consent, unless expressly allowed by a stated permitted purpose.

- Permitted purposes include protecting data security, complying with legal obligations, effectuating a product recall or fulfilling a warranty, conducting market research and medical research (which requires affirmative express consent for consumer participation), de-identifying data for use in product improvement and research, to prevent fraud and harassment, to respond to ongoing or imminent security incidents or public safety incidents, and to process previously collected non-sensitive covered data for advertising.
- The FTC shall issue guidance regarding what is reasonably necessary and proportionate to comply with data minimization under this title.
- Nothing in the title shall be construed to diminish First Amendment freedoms.

PRIVACY BY DESIGN:

- Covered entities and service providers shall establish, implement, and maintain reasonable policies, practices, and procedures that reflect the role of the covered entity or service provider in the collection, processing, retention, and transferring of covered data.

TRANSPARENCY:

- Covered entities and service providers must have publicly available privacy policies detailing their data privacy and security practices.
- 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; a description for how the covered entity treats information from covered minors differently that other covered data; data security practices; and the effective date of the privacy policy.
- Privacy policies must prominently describe how consumers can exercise their individual controls and opt-out rights. The policy must be accessible in multiple languages and to people living with disabilities.
- When a covered entity makes a material change to its policy, it must provide advanced notice and means to opt out of the processing or transfer of previously collected data.
- Large data holders are subject to additional requirements pursuant to retaining and publishing their privacy policies from the past 10 years and also providing a short-form notice of their policies.

CONSUMER CONTROLS OVER COVERED DATA:

- Consumers have the right to access their covered data, after submitting a verifiable request, that is collected, processed, or retained by a covered entity 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, a covered entity must correct inaccurate or incomplete covered data with respect to an individual.
- Upon a verified request, a covered entity must delete the covered data of an individual.
- Upon a verified request, a covered entity must export covered data pertaining to an individual to the extent technically feasible.
- Parents are able to exercise such rights on behalf of a child under the age of 13.

- Covered entities must comply with individual control rights within specified timeframes, and large data holders must report metrics related to the requests they process.
- Covered entities must ensure that rights are accessible to individuals living with disabilities and available in any language in which the entity provides a product or service.
- The FTC is directed to issue guidance for this section.
- Covered entities shall deny an individual's request if it would require access to data about another individual, interfere with lawful legal process, violate another law, and other exceptions.
- Covered entities may deny an individual's request if the request would be demonstrably impossible, would require deleting data necessary to perform a contract, would require the release of trade secrets, would delete certain covered data that relates to a public figure, would delete covered data that the entity believes may be evidence of an abuse of the covered entity's product or services, or would prevent the maintenance of a confidential record of opt out rights. The FTC may promulgate rules to expand the situations where an entity may deny a request.

OPT OUT RIGHTS AND UNIVERSAL OPT OUT MECHANISM:

- A consumer has the right to opt out of the transfer of non-sensitive covered data to a third party.
- A consumer has the right to opt out of targeted advertising as it relates to non-first party relationships and high-impact social media companies.
- The FTC is directed to issue regulations to establish the requirements and technical specifications for one or more centralized mechanisms for individuals to exercise the opt out rights.

INTERFERENCE WITH CONSUMER RIGHTS:

- Covered entities are prohibited from using dark patterns to divert an individual's attention from notice required by the title, impair the exercise of any right under the title, or to obtain consent under the title.
- A covered entity shall not condition the exercise of a right described in this title through the use of any false, fictitious, fraudulent, or materially misleading statement or representation.

PROHIBITION ON DENIAL OF SERVICE AND WAIVER OF RIGHTS:

- Covered entities may not retaliate against individuals for exercising their rights under the title, including by denying or charging different rates for goods or services.
- Covered entities may offer bona fide loyalty programs or market research opportunities to consumers.
- Covered entities must obtain the consumer's affirmative express consent for participation in a bona fide loyalty program.

DATA SECURITY AND PROTECTION OF COVERED DATA:

- Covered entities and service providers must 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 of safeguards.
- Covered entities and service providers must assess vulnerabilities and mitigate reasonably foreseeable risks to consumer data. The FTC shall enact rules to interpret this section in consultation with the Department of Commerce.

EXECUTIVE RESPONSIBILITY:

- All covered entities must designate one or more covered employees to serve as privacy and data security officers.
- Large data holders are required to designate both a privacy and a data security officer.
- Large data holders are also directed to file with the FTC annual certifications of internal controls designed to comply with the title and internal reporting structures for compliance with the title.
- Large data holders must conduct privacy impact assessments on a biennial basis.

SERVICE PROVIDERS AND THIRD PARTIES:

- Service providers must adhere to the instructions of a covered entity and assist the entity in fulfilling its obligations under the title.
- Service providers must cease data practices where they have actual knowledge or reason to believe that a covered entity is in violation of this title.
- Service providers must 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.

DATA BROKERS:

- Data brokers must 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 FTC's data broker registry website. The website must be reasonably accessible for individuals living with disabilities.
- Data brokers are prohibited from advertising data for the purpose of stalking or fraudulent purposes and are prohibited from misrepresenting their business practices.
- The FTC is 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" and "delete my data" mechanism for consumers to use. The FTC shall also issue guidance regarding the content of a data broker's website.

COMMISSION-APPROVED COMPLIANCE GUIDELINES:

- The FTC shall approve compliance guidelines related to the handling of covered data that would apply to covered entities but not large data holders or data brokers.
- Applications for compliance guidelines must meet or exceed the requirements of this title and shall identify an independent organization responsible for administering the guidelines.
- The FTC is directed to approve or deny applications within one year and may withdraw approval of guidelines if they no longer meet the requirements of this title.
- Covered entities participating in guidelines must self-certify compliance and identify the independent organization overseeing their compliance.
- Participation in FTC-approved guidelines entitles a covered entity to a rebuttable presumption of compliance with the title.

PRIVACY-ENHANCING AUDITS PILOT PROGRAM:

- Establishes 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 title.
- Participation in the pilot program entitles a covered entity to a rebuttable presumption of compliance with the data security requirements of this title for a private right of action related to a data breach.

ENFORCEMENT BY THE FEDERAL TRADE COMMISSION:

- The title provides for FTC enforcement.
- The FTC is directed to establish a new bureau comparable to the Bureaus of Enforcement and Competition to carry out its authority under the title.
- Violations of the title will be treated as violations of a rule defining an unfair or deceptive practice under the FTC Act.
- A Privacy and Security Victims Relief Fund is established from which the FTC is to provide redress to persons affected by an act or practice in violation of the title.
- The FTC is directed to issue a report to Congress detailing its enforcement and administration of the title.

ENFORCEMENT BY STATE ATTORNEYS GENERAL:

- The title authorizes enforcement by State attorneys general, chief consumer protection officers, and other officers of a State in federal district court.
- States may seek injunctive relief; civil penalties, damages, restitution, or other consumer compensation; attorneys' fees and other litigation costs; and other relief as appropriate.
- State attorneys general must notify the FTC prior to initiating an action under this title.
- The GAO is directed to study the practice of hiring external counsel by State attorneys general.

ENFORCEMENT BY INDIVIDUALS:

- Consumers may file private lawsuits against entities that violate their rights under this title.
- An action for a substantial privacy harm or by a minor shall not be subject to mandatory arbitration.
- A person bringing an action may recover actual damages, injunctive relief, declaratory relief, and reasonable attorney fees and costs. Any amount that a court orders an entity to pay may be offset by recovery for the same violation pursuant to an FTC or state action.
- A person may recover statutory damages consistent with Illinois's Biometric Information Privacy Act and Genetic Information Privacy Act for an action involving a violation of the affirmative express consent provisions for biometric and genetic information where the conduct occurred substantially and primarily in Illinois.
- A person who is a resident of California may recover statutory damages consistent with the California Privacy Rights Act for an action related a data breach.
- Entities are provided an opportunity to cure in actions requesting injunctive relief and written notice in actions seeking actual damages with the ability to settle any potential violation, except for actions for a substantial privacy harm.
- If a person, or their representative, brings an action seeking actual damages without first issuing the proper notice, the action may be dismissed without prejudice and shall not be reinstated until such person has complied with such notice requirements.

PREEMPTION:

- State laws covered by the title are preempted, with the exception of an enumerated list of State laws: consumer protection laws; civil rights laws; provisions of laws that address the privacy of employees; provisions of laws that address privacy of students; provisions of laws that address data breach notification; contract or tort laws; criminal laws; criminal and civil laws on cyberstalking and blackmail; public safety laws unrelated to privacy; provisions of laws that address public records laws; provisions of laws that address banking and financial records; provisions of laws that address electronic surveillance and wiretapping; provisions of laws that address unsolicited email and phone laws; provisions of laws that address health care, health information, and medical information; provisions of laws governing the confidentiality of library records; and provisions of laws that address encryption.
- State laws that provide protections for children or teens shall be preempted only to the extent that such laws are in conflict with a provision of this title, unless otherwise providing greater protections.
- Federal laws, including laws regarding information security breaches of common carriers and antitrust laws, are not limited except where specified in the title.
- To the extent that a covered entity or service provider is required to comply with certain other privacy and data security laws and regulations, it shall not be subject to this title with respect to the activities governed by those privacy and data security laws and regulations.
- Federal and State common law and statutory causes of action for civil relief are preserved under this title.
- Certain FCC privacy laws and regulations shall not apply to covered entities or service providers with respect to data privacy and security obligations, to the extent those provisions govern the collection, processing, retention, or transferring of covered data.

DATA PROTECTIONS FOR COVERED MINORS:

- A covered entity or service provider may not engage in targeted advertising or first party advertising to a covered minor if such entity has knowledge that the individual is a covered minor, except that a covered entity or service provider may display to a covered minor age-appropriate advertisements intended for an audience of covered minors, so long as the covered entity or service provider does not use any covered data other than whether the individual that receives the advertisement is a covered minor.
- A covered entity or service provider may not transfer the covered data of a covered minor to a third party other than for permitted exceptions.
- The commission may conduct a rulemaking to establish a process for parents and teens to exercise the rights provided to them in this title with respect to covered entities and data brokers. Any such rulemaking should take into account the specific needs of parents, children, and teens and should consider how best to harmonize the processes provided for under this title with the processes and guidance provided for under Title II and by the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et. seq) and any rulemakings undertaken by the Commission thereunder. It should also consider options for reducing undue burdens on parents, children, teens, covered entities, and data brokers.

TERMINATION OF FTC RULEMAKING ON COMMERCIAL SURVEILLANCE AND DATA SECURITY:

- Terminates the FTC's Rulemaking on Commercial Surveillance and Data Security on the date of enactment of this title.

SEVERABILITY:

- Any finding that a provision of this title is invalid shall not apply to the remainder of the title.

EFFECTIVE DATE:

- The title shall take effect 180 days after enactment.

TITLE II:

This title amends the Children's Online Privacy Protection Act of 1998 by:

- Amending definitions of Operator; Personal Information; Support for the Internal Operations of a Website, Online Service, Online Application, or Mobile Application; and Verifiable Consent.
- Adds new definitions for the terms Connected Device, Online Application, Mobile Application, Precise Geolocation Information, and Educational Agency or Institution.
- Extends the additions of online application and mobile application definitions to the list of platforms directed to children and covered in this Act.
- Amending the knowledge standard in current law to "actual knowledge or knowledge fairly implied on the basis of objective circumstances."
- Allowing operators working with educational institutions to have certain exceptions.
- Granting parents the right to terminate services directed at their children.
- Directing the FTC to explore common verifiable consent mechanisms.

- Preempting State laws that conflict with the purposes of this title, unless providing greater protections to children.
- Amending the safe harbor options for entities and directing the Inspector General to analyze whether the safe harbor provisions are operating fairly and effectively in specific regard to protecting the interests of children.
- Directing the FTC to report on platforms compliance and actions, investigations, and complaints received alleging violations of the Act.