Congress to Consider Comprehensive Federal Data Privacy Law

07.28.2022

ATTORNEYS

Maureen E. Fulton

Mikaela M. Witherspoon

PRACTICE AREAS

Data Privacy and Security

Introduction

Newly proposed legislation in the U.S. House of Representatives marks a significant step toward comprehensive, nationwide privacy legislation. The bill, H.R. 8152, also known as the American Data Privacy and Protection Act (the "Act"), was officially introduced on June 21, 2022 and would generally prohibit the collection, processing, and transfer of covered personal information. It would also establish requirements for covered entities regarding their privacy policies and practices. Further, the bill would allow for enforcement by the Federal Trade Commission ("FTC"), state attorneys general and privacy authorities, and private individuals.

While significant steps remain for its passage in the House, the Act is the most traction a federal privacy bill has gained in the years that Congress has considered such legislation. The bill was amended by the House Committee on Energy and Commerce and forwarded to the full House of Representatives on July 20, 2022, where it awaits further debate.

Scope of the Act

Personal Information Subject to the Act

The Act would cover information that identifies, or is linkable to, an individual, or information from a device that identifies, or is linkable to, an individual. This would encompass derived data, such as a synthesis of previously collected data to reveal customer preferences based on demographic information, and unique identifiers, such as IP addresses, cookies, and pixel tags.

Congress to Consider Comprehensive Federal Data Privacy Law

The Act would not cover de-identified data, employee data, or publicly available information.

Under the Act, government-issued identifiers like Social Security Numbers and driver's license numbers, financial account information, precise geolocation information, information about minors under age 17, and several other expressly defined data types (called "sensitive covered data" by the Act), would be subject to enhanced restrictions on their use and transfer to other entities.

Entities Subject to the Act
The Act would broadly apply to any entity or person that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data, and is either (1) subject to the FTC Act, (2) a common carrier subject to the Communications Act of 1934, or (3) a non-profit. The Act would also apply to any entity or person that controls, is controlled by, or is under common control with another covered entity.

The Act would not apply to individuals acting in a non-commercial context, governmental entities, a person or entity acting on behalf of a governmental entity. Small businesses, as defined by the Act, would be exempt from certain requirements, including several of the data security practices required of other entities.

A few categories of entities in the Act are especially worth noting:

Large Data Holders
A covered entity would be considered a "large data holder" if, in the most recent calendar year, it had annual gross revenue of $250 million or more, and collected, processed, or transferred: (1) the covered data of five (5) million or more individuals or devices linkable to individuals, and (2) the sensitive covered data of more than 200,000 individuals or devices linkable to individuals.

There are exceptions to what constitutes a large data holder. Data collected and processed solely for the purpose of conducting a transaction for a product or service requested by an individual would be excluded from the overall count. Additionally, an entity that would meet the large data holder threshold solely on the basis of collecting or processing personal email addresses, phone numbers, or log-in information of an individual used to access an entity-administered account, would not be considered a large data holder for purposes of this bill.

Third-Party Collecting Entity
An entity subject to the Act is considered a "third-party collecting entity" if its principal source of revenue is derived from processing or transferring covered data that the entity did not collect directly from the individuals to whom the data is linked or linkable, such as a data broker. This would not apply to an entity acting as a service provider, as defined by the Act.

Congress to Consider Comprehensive Federal Data Privacy Law

High-Impact Social Media Company

The Act places enhanced requirements on entities that (1) generate at least $3 billion in annual revenue; and (2) provide an internet-accessible platform that is primarily used for accessing and sharing user-generated content with at least 300 million monthly active users in at least three (3) of the preceding 12 months.

Service Providers

The Act defines service providers as a person or entity that collects, processes, or transfers covered data on behalf of, and at the direction of, a covered entity or governmental entity. An entity acting solely as a service provider would not be considered a "covered entity" for purposes of the Act. Therefore, to the extent certain provisions of the Act only refer to "covered entities," service providers would not be subject to those requirements. However, the Act does still apply to service providers, in general.

Restrictions and Permissible Use of Covered Data

The Act prohibits covered entities from collecting, processing, or transferring covered data, unless such collecting, processing, or transferring is limited to what is reasonably necessary to (1) provide or maintain a product or service requested by the individual to whom the data pertains, or (2) effect another purpose expressly permitted by the Act. In its current form, the Act contains 17 expressly permissible purposes, including:

- Completion of routine administrative, operational, and accounting activity associated with the product or service requested by an individual;
- Performing system maintenance and inventory management;
- Development, maintenance, or enhancement of a product or service for which the data was collected;
- Prevention and detection of illegal activity, data breaches, or other security incidents;
- Compliance with legal obligations;
- Transferring assets to a third party in the context of a merger, acquisition, bankruptcy, or similar transaction;
- Providing first party advertising or marketing of products or services to individuals who are not covered minors; and
- Providing targeted advertising that complies with the Act's requirements regarding targeted advertising.

Congress to Consider Comprehensive Federal Data Privacy Law

Requirements for Entities Subject to the Act

The Act would establish several requirements for covered entities. All such entities would be required to establish reasonable policies, practices, and procedures regarding data collection to mitigate privacy risks and promote compliance. This includes sufficient security measures to protect against unauthorized access to, and acquisition of, data. Such security measures would include, at minimum, risk and vulnerability assessment, corrective action to mitigate identified risks and vulnerabilities, properly disposing of data, employee training, and implementing data breach response protocols.

Additional requirements include:

- Businesses would be required to make their privacy policies publicly available;
- Businesses would be required to assess the design, structure, and inputs of any algorithms used for data collection, processing, or transfer;
- Businesses, except for small businesses, would be required to conduct a biennial privacy impact assessment, and to produce and retain a corresponding privacy impact report;
- Large data holders would be required to provide a short-form notice of their privacy and data practices;
- Third-party collecting entities, specifically, would be required to place a clear notice on its website that it is a third-party collecting entity; and
- Third-party collecting entities meeting certain criteria would be required to register with the FTC annually.

Consumer Rights

The Act would provide individuals with the right to access, correct, delete, and obtain portable copies of, their covered data. Covered entities would be required to provide the opportunity to exercise each right free-of-charge, unless the individual submits more than two (2) requests in any 12-month period, in which case a reasonable fee could be charged.

The Act also contains opt-out rights related to first-party marketing and targeted advertising. First, individuals would have the right to opt-out of the transfer of covered data that is done for the purpose of providing first-party marketing of products or services provided by the business. Second, individuals would have the right to opt-out of targeted advertising from the business, which is defined by the Act as delivering an online advertisement to an individual, or device identified by a unique identifier, based on known or predicted preferences, characteristics, or interests associated with the individual or uniquely identified device.

Congress to Consider Comprehensive Federal Data Privacy Law

The Act prohibits targeted advertising to minors if the business has knowledge that the individual is a minor. The term "targeted advertising" does not include advertising or marketing in response to an individual's request for information, or contextual advertising, which is based on the content in which the advertisement appears rather than the individual viewing the advertisement.

Right to Access
Access would need to be granted to the covered data of the individual making the request, except data in a back-up or archival system, that is collected, processed, or transferred by the covered entity or any service provider of the covered entity within the 24 months preceding the request.

Right to Correct
Any verifiable and substantial inaccuracy or incomplete information would need to be corrected upon request, and the covered entity would need to make reasonable efforts to notify all relevant third parties or service providers of the corrected information.

Right to Delete
Deletion of an individual's covered data would need to be completed upon request, and the covered entity would need to make reasonable efforts to notify all relevant third parties or service providers of the deletion request.

Right to Obtain Copies
To the extent technically feasible, covered entities would need to export covered data to the individual or directly to another entity upon request. Such export would need to be in a portable, structured, and machine-readable format.

Enforcement

The Act would establish the Bureau of Privacy within the FTC, which would be tasked with carrying out the duties of the FTC under the Act, including enforcement. In addition to civil enforcement by the FTC and state attorneys general or state privacy authorities, the Act would create a private right of action, allowing individuals to sue a covered entity alleged to have violated the Act. The Act would provide the right to both monetary and non-monetary relief for successful plaintiffs. The private right of action would become effective two (2) years following the effective date of the Act.

The Act would also preempt state laws that are covered by the Act or a regulation promulgated under the Act, with many exceptions. State consumer protection laws of general applicability, criminal laws, civil laws regarding child abuse or trafficking, and several other types of laws would not be preempted by the Act. This will be a highly negotiated issue, as members of

Congress to Consider Comprehensive Federal Data Privacy Law

Congress are divided as to whether a federal privacy law should be a governing standard to replace a patchwork of state privacy laws, or serve as a "floor" of minimum protections that states are free to go beyond as they see fit. California lawmakers, in particular, are concerned with the Act's preemption of state privacy laws, as they believe the Act in its current form provides lesser protection for individuals than the newly enacted California Privacy Rights Act (CPRA), which is set to go into effect on January 1, 2023.

Koley Jessen will continue to monitor developments related to the American Data Privacy and Protection Act and advise as updates become available. If you have questions about the Act, please contact one of the specialists in Koley Jessen's **Data Privacy and Security Practice** Area.

Special thanks to Jacob Bishop, Koley Jessen Summer Associate, for his contributions to this article.