HINSHAW

Alerts

Privacy Bill Essentials: A Federal Information Transparency and Personal Data Control Act

March 16, 2021
Hinshaw Privacy & Cyber Bytes

On March 10, 2021, Representative Suzan DelBene (D-WA) re-introduced the Information Transparency and Personal Data Control Act (the Bill) in an effort to provide a uniform national consumer data privacy standard in place of the patchwork of conflicting state laws already in place and soon to become law.

The Bill intends to protect the sensitive personal information of individuals by requiring companies to obtain opt-in consent from persons prior to collecting, using, sharing, selling, or disclosing their sensitive personal information. While previous versions of the Bill stalled, there is a sense of optimism that this version may become law in the current Congress and Administration. The Bill has been endorsed by a number of business trade groups, including the U.S. Chamber of Commerce.

To whom would it apply?

The Bill applies to "controllers, processors, and third parties" who collect, transmit, store, process, sell, or share sensitive personal information from persons operating in, or located in, the United States at the time of the collection, transmission, storage, processing, sale, or sharing.

- A controller is "a person that, on its own or jointly with other entities, determines the purposes and means of processing sensitive personal information."
- A processor is "a person that processes data on behalf of a controller or another processor according to and for the purposes set forth in the documented instructions."
- Notably, a person who processes data on its own behalf or for its own purposes is not considered a processor with respect to that data, but is instead a controller.
- A third-party is defined as "an individual or entity that uses or receives sensitive personal information obtained by or on behalf of a controller," with limited exceptions set forth in the Bill.

Service Areas

Privacy, Security & Artificial Intelligence

What types of information would it cover?

The sensitive personal information covered in the Bill includes:

- financial account numbers;
- health information;
- genetic data;
- Information pertaining to children under 13 years of age;
- Social Security numbers;
- unique government-issued identifiers;
- authentication credentials for a financial account (e.g. username and password);
- precise geolocation information;
- content of a personal wire communication, oral communication, or electronic communication such as e-mail or direct messaging with respect to any entity that is not the intended recipient of the communication;
- call detail records for calls conducted in a personal and not a business capacity;
- biometric information;
- sexual orientation, gender identity, or intersex status;
- citizenship or immigration status;
- mental or physical health diagnosis;
- religious beliefs; and
- web browsing history, application usage history, and the functional equivalent of either that is data described in this subparagraph that is not aggregated data.

Sensitive information does not include de-identified information, employment information, certain business communications that contain personal information, and publicly available information.

What rights would it create?

The Bill would give persons operating or located in the United States the right to:

- Opt-in before their sensitive personal information is collected, transmitted, stored, processed, sold, or otherwise shared
- Opt-out with respect to the collection, transmission, storage, processing, selling, and other use of their non-personal information

The opt-in consent would not be required when the processing of sensitive personal information is consistent with the controller's relationship with the user. For example, to carry out the term of the contract or service, to accept and process payments, and to complete transactions, among other uses.

What obligations would it impose?

- Controllers must provide a specific opt-in notice to users whose sensitive personal information is collected, transmitted, stored, processed, sold, or otherwise shared
- Processors and third parties shall note use or disclose the sensitive personal information in any way that exceeds the limits of consent
- Controllers, processors, and third parties would need to publicly post a "transparent privacy, security, and data use policy" that:
  - Uses concise and plain language

- Is clear and conspicuous
- Uses visualizations for complex information
- Is free of charge

- The posted policy must:
  - Identify the entity collecting or processing the sensitive personal information
  - Provide contact information for that entity
  - Identify the purpose for collecting, storing, processing, selling, sharing, or otherwise using the sensitive personal information
  - Identify the categories of third persons with whom the information will be shared and for what general purposes
  - Provide a process for individuals to withdraw consent
  - Provide a process for individuals to view the information
  - Identify the categories of sensitive personal information that is collected and shared
  - Identify how sensitive personal information is protected from unauthorized access or acquisition

- Controllers, processors, and third parties would need to obtain a privacy audit from a qualified, objective, independent third-party every two years, and:
  - Post a notice of whether they were found to be compliant
  - Provide the report to the Federal Trade Commission (FTC)

The Bill provides for a Small Business Audit Exemption, meaning that entities who collect, store, process, sell, share, or use sensitive personal information relating to 250,000 individuals or less per year are not required to submit a privacy audit.

The Bill's requirements do not apply when the personal information is used for certain purposes such as preventing and detecting fraud or crime, responding to valid legal processes, or using data in a way that is authorized by the Fair Credit Reporting Act, among other purposes.

How would it be enforced?

State attorney generals and the FTC would have powers to enforce the law through the privacy audits. Further, the FTC will have rule-making authority to issue additional regulations. Unlike previous versions of the Bill, this one does not include a private right of action that would allow consumers to file lawsuits against companies over privacy violations. Instead, this version of the Bill permits a state attorney general to bring a cause of action on behalf of consumers. While the Bill is silent as to fines or penalties for violating the law, there remains the possibility that the FTC could establish fines or penalties pursuant to the rule-making authority granted to it.

When would it go into effect?

Should the Bill be signed into law, it would go into effect 180 days after it is enacted.

Where does it stand?

The Bill was introduced on March 10, 2021 in the House of Representatives. To date, it has 15 Democratic cosponsors. In the past, Democrats and Republicans have disagreed on certain provisions in similar bills that had been introduced in Congress such as provisions on preemption, states' rights, and a private cause of action. Given that this version of the Bill is seen as more business-friendly than previous versions, there is a chance that some Republicans will cosponsor the Bill.