HINSHAW

Alerts

Privacy Bill Essentials: Proposed Federal "Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act"

August 6, 2021
Hinshaw Privacy & Cyber Bytes

U.S. Senators Roger Wicker (R-Miss) and Marsha Blackburn (R-Tenn) recently reintroduced a comprehensive federal privacy bill entitled the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act. The SAFE DATA Act integrates themes from three previously introduced legislative proposals: the discussion draft of the U.S. Consumer Data Protection Act (CDPA), the Filter Bubble Transparency (FBT) Act, and the Deceptive Experiences To Online Users Reduction (DETOUR) Act.

If signed into law, the SAFE DATA Act would create a single federal standard for consumer data privacy and preempt all state consumer data privacy laws.

To whom would it apply?

The SAFE DATA Act aims to protect the personal data of all individuals residing in the U.S. and would apply to all businesses under the purview of the Federal Trade Commission (FTC), as well as non-profits and common carriers. Small businesses are exempt from complying with various provisions of the SAFE DATA Act (*e.g.*, sections 103, 105, and 301) if they can establish that for the three preceding calendar years: their revenues did not exceed $50 million; they processed covered data of less than 1,000,000 individuals; they never employed more than 500 individuals at any one time; and, they derived less than 50% of their revenues from transferring covered data.

What types of information would it cover?

The SAFE DATA Act defines covered data as that which "identifies or is linked or reasonably linkable to an individual or a device that is linked or reasonably linkable to an individual." Falling under this broad definition is sensitive data, which includes social security numbers; passport numbers; data that describes or reveals the diagnosis and treatment of past, present, or future physical health, mental health, or the disability of an individual; financial account numbers; biometric information; geolocation information; private communications, such as emails; data revealing sexual orientation or behavior; and data about the online activities of an individual.

Attorneys

Jason J. Oliveri

Service Areas

Privacy, Security & Artificial Intelligence

Excluded from the definition of covered data is aggregated data, de-identified data, employee data, and publicly available information.

What rights would it create?

The SAFE DATA Act would provide individuals with the right to:

- Know what categories of covered data are being collected and the purpose for collection;
- Access the categories of covered data collected and the categories of covered data disclosed to third parties;
- Ensure that the covered data collected is accurate, and if not, correct it;
- Erase or delete the covered data collected; and
- Obtain covered data collected in a machine-readable, structured, and portable format that is not subject to any licensing restrictions.

What obligations would it impose?

The key requirements for covered businesses derived from the CDPA are:

- Publish a transparent privacy policy clearly and conspicuously in all languages the business uses to provide a service or product that is disclosed prior to or at the point of covered data collection;
- Obtain affirmative, express consent before transferring or processing sensitive data. If the business has actual knowledge that an individual is between the ages of 13 and 16, it must obtain affirmative, express consent from a parent or guardian prior to transferring covered data to a third-party;
- Provide each individual the ability to opt-out of the collection, processing, or transfer of such individual's covered data before such collection, processing, or transfer occurs;
- Continue to provide products and services to individuals who exercise their rights under the SAFE DATA Act;
- Collect, process, and transfer covered data only to the extent reasonably necessary and proportionate to provide or improve a product or service, or a communication about a product or service;
- Perform a privacy impact assessment within a year of enactment of the SAFE DATA Act, and then no less frequently than once every two years if, in the most recent calendar year, the business processed or transferred the covered data of more than 8,000,000 individuals or the sensitive data of more than 300,000 individuals; and
- Maintain a reasonable data security program to protect the confidentiality, security, and integrity of covered data.

The key requirements for covered businesses derived from the FBT Act are:

- Provide a clear and conspicuous notice to users of a platform that uses an "opaque algorithm" that makes inferences based on user-specific data to select the content the user sees; and
- Provide users with a version of the platform that uses an "input-transparent algorithm" and enables users to easily switch between the version of the platform that uses an "opaque algorithm."

The key requirements for covered businesses derived from the DETOUR Act are:

- Design platforms in a manner so that users are not manipulated into consenting to the use of their data or in a manner that cultivates "compulsive usage" in users who are below the age of 13; and
- Obtain informed consent for behavioral or psychological studies of customer segments.

How would it be enforced?

The SAFE DATA Act designates the FTC as the federal agency responsible for enforcing the act in the same manner, and by the same means as it enforces the Federal Trade Commission Act (FTCA). This means violators will face the same penalties and be granted the same immunities as those provided in the FTCA.

State Attorneys General may also commence a civil action in federal court on behalf of the residents of their state to the extent it has reason to believe that a business is engaging in an act or practice in violation of the SAFE DATA Act that threatens the interests of residents. The State Attorney General may seek, among other forms of relief, damages, civil penalties, restitution, and other compensation on behalf of the residents of the state.

The SAFE DATA Act does not provide for a private right of action. It would go into effect 18 months after enactment.