HINSHAW

Alerts

Privacy Bill Essentials: Proposed Federal Consumer Data Privacy and Security Act

May 5, 2021
Hinshaw Privacy & Cyber Bytes

On April 29, 2021, Senator Jerry Moran of Kansas reintroduced a comprehensive federal privacy bill entitled the Consumer Data Privacy and Security Act (the Act). The Act integrates themes from the CCPA and GDPR and provides similar rights and protections, but is more favorable to small and midsize businesses. If signed into law, the 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 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 as well as non-profits and common carriers. Small businesses are exempt from complying with an individual's right to access and rights to accuracy and correction. To qualify for the exemption, the business must:

- Have no more than 500 employees;
- Maintain less than $50,000,000 in average gross receipts for the previous three years; and
- Collect and process the personal data of no more than 1,000,000 individuals.

Service providers (*i.e.*, a business that operates under a contract with the business from which it receives personal information) are exempt. However, at the end of the contract or service, the service provider must delete, de-identify, or return the personal data to the business with which it contracted.

What types of information would it cover?

The Act broadly defines personal data to mean information that "identifies or is linked or reasonably linkable to a specific person." This would include, but is not limited to, a consumer's real name, postal address, account name, email address, social security number, driver's license number, or passport number.

Attorneys

Jason J. Oliveri

Service Areas

Privacy, Security & Artificial Intelligence

What rights would it create?

The Act would provide individuals with the right to:

- Know what categories of personal data are being collected and the reason why they are being collected;
- Access the categories of personal data collected and the categories of personal data disclosed to third parties;
- Ensure that the personal data collected is accurate, and if not, correct it;
- Erase or delete the personal data collected; and
- Export the personal data generated in a machine-readable format and to transmit that information to another entity.

What obligations would it impose?

The Act would require a business that collects personal data to:

- Provide notice in a prominent and easy to understand format the types of personal data the business collects and the purpose for its collection;
- Obtain either explicit or implicit consent prior to collecting personal data. Consent will be implied where the individual did not decline the collection request and a reasonable amount of time has passed;
- Make publicly available its past and present privacy policies in a clear and prominent location;
- Provide each individual whose personal data has been collected with a clear and easy to use means to exercise their rights under the Act;
- Maintain a comprehensive data security program that contains safeguards to protect the security, confidentiality, and integrity of the personal data collected;
- Ensure that service providers have established appropriate privacy and security procedures and controls; and
- Designate a privacy officer whose job it is to oversee its policies and practices related to the collection of personal data.

Businesses may collect personal data without consent to the extent reasonably necessary and for a permissible purpose. The Act establishes the following permissible purposes: (1) provision of service or performance of a contract; (2) compliance with laws; (3) to prevent immediate danger to the personal safety of any individual (including to effectuate a product recall); (4) to prevent fraud and protect the security of the covered entity's, service providers', or individual's rights, property, services, or information systems; (5) research performed by the covered entity or service provider (at the direction of the covered entity); and (6) the covered entity's or service provider's operational purposes.

How would it be enforced?

The Act designates the Federal Trade Commission as the federal agency responsible for administering the Act and grants it rule-making. A business that violates the Act would be subject to civil penalties amounting to the number of individuals affected multiplied by an amount not to exceed $42,530. In considering the penalty, the following factors will be taken into account: (1) the degree of harm; (2) the intent of the business; (3) the size and complexity of the business; (4) the controls put in place by the business; (5) whether the business self-reported; and (6) the mitigation efforts of the business.

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 Act that threatens the interests of residents.