HINSHAW

Alerts

Privacy Bill Essentials: Proposed Connecticut Consumer Privacy Act (S.B. 893)

April 20, 2021 | Updated June 28, 2021
Hinshaw Privacy & Cyber Bytes

Update: Like several other state privacy bills introduced this year, SB 893 died in chamber.

Connecticut is the latest state to introduce consumer privacy legislation. If enacted, the Connecticut Act Concerning Consumer Privacy (The Act) would join the existing nationwide patchwork of state privacy laws. The Act would establish a framework for controlling and processing personal data, and include the now-typical consumer rights to access, correct, delete, and know how businesses are using their personal data. The current draft also includes an opt-out for targeted advertising. It does not, however, contain a private right of action.

To whom would it apply?

The Act would apply to persons that conduct business in Connecticut or produce products or services that are targeted to residents of Connecticut that:

- During a calendar year, control or process the personal data of not less than 100,000 consumers; OR
- Control or process the personal data of not less than 25,000 consumers and derive more than 50% of their gross revenue from the sale of personal data.

"Controller" would mean a natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data.

"Processor" means a natural or legal entity that processes personal data on behalf of a controller.

The Act would not apply to:

- State boards, bureaus, commissions, districts, agencies, and political subdivisions;
- Financial institution or data subject to GLBA;
- Covered entities and business associates governed under HIPAA;
- Nonprofit organizations; and
- Higher education institutions

Service Areas

Privacy, Security & Artificial Intelligence

What types of information would it cover?

"Personal data" would mean any information that is linked or reasonably linkable to an identified or identifiable natural person. It would not include de-identified data or publicly available information.

"Sensitive data" would mean personal data that includes:

- Data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation or citizenship or immigration status;
- The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
- Personal data collected from a known child; or
- Precise geolocation data.

In a departure from other consumer privacy laws, the term "Sale" is more narrowly defined. "Sale of personal data" means the exchange of personal data for monetary consideration by the controller to a third party. The Act would expressly exclude the following actions from the definition:

- Disclosure of personal data to a processor that processes the personal data on behalf of the controller;
- Disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;
- Disclosure or transfer of personal data to an affiliate of the controller;
- Disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media, and (ii) did not restrict to a specific audience; and
- Disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the controller's assets.

What rights would it create?

"Consumer" means a natural person who is a resident of Connecticut and acting only in an individual or household context. Consumers would have the right to:

- Request whether a controller is processing the consumer's personal data;
- Request access to such personal data;
- Request to correct inaccuracies in the consumer's personal data;
- Request to delete personal data provided by, or obtained about, the consumer;
- Request a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format; and
- Optout of the processing of the personal data for purposes of:
  - Targeted advertising;
  - The sale of personal data; or
  - Profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

What obligations would it impose?

In addition to other obligations not identified here, Controllers would be required to do the following:

- Limit the collection of personal data to what is "adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed";
- Provide a reasonably accessible, clear, and meaningful privacy notice that must include:
  - The categories of personal data processed by the controller;
  - The purpose for processing personal data;

    - How consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision about the consumer's request;
    - The categories of personal data that the controller shares with third parties, if any; and
    - The categories of third parties, if any, with which the controller shares personal data.
- Clearly and conspicuously disclose the manner in which the controller sells personal data to third parties or processes personal data for targeted advertising;
- Respond to verified consumer requests twice annually, free of charge;
- Establish, implement and maintain reasonable administrative, technical and physical data security practices;
- Conduct and document a data protection assessment for
    - Processing personal data for targeted advertising purposes:
    - Selling personal data:
    - Processing sensitive data: and
    - Processing activities involving personal data that present a heightened risk of harm to consumers.
- Not process sensitive data concerning a consumer without obtaining the consumer's consent:
- Not discriminate; and
- Establish binding contracts with processors that clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties.

The obligations, however, would not restrict a controller's ability to:

- Comply with federal, state, or municipal ordinances or regulations;
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, municipal, or other governmental authorities;
- Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or municipal ordinances or regulations;
- Investigate, establish, exercise, prepare for or defend legal claims;
- Provide a product or service specifically requested by a consumer;
- Perform a contract to which a consumer is a party, including fulfilling the terms of a written warranty;
- Take steps at the request of a consumer prior to entering into a contract;
- Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;
- Prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;
- Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entities; or
- Assist another controller, processor, or third party with any of the obligations under the Act.

The obligations would not apply if compliance would violate an evidentiary privilege under Connecticut law.

How would it be enforced?

The Attorney General would have exclusive authority to enforce violations. The Attorney General may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General. The disclosure of an assessment would not constitute a waiver of attorney-client privilege or work-product protection, and would be considered confidential and exempt from disclosure pursuant to a Freedom of Information Act request.

The Act would permit a 30 day cure period after notice of a violation and provide for a civil fine of up to $7,500 per violation.

There would be no private right of action under the Act.

When would it go into effect?

If enacted, the Act would become operative on January 1, 2023.

Where does it stand?

The Act was reported out of the Legislative Commissioner's Office on April 8, 2021, and is tabled for the calendar.