HINSHAW

Privacy Bill Essentials: Utah

Privacy, Cyber & AI Decoded Alert | 3 min read
Feb 23, 2021

** Update: Utah's Senate Bill 200 passed each of its first two Senate floor readings, but failed to get a required third reading on the final day it was able to pass the chamber before the end of the Utah legislative session on March 5, 2021.*

On February 16, 2021, Senator Kirk Cullimore introduced the Utah Consumer Privacy Act in the Utah State Senate. The bill would provide consumers the right to access, correct, and delete certain personal data, as well as the right to opt out of collection and use personal information for certain purposes. In addition, the bill features mandated annual data protection assessments, but no private right of action.

To whom would it apply?

The Act would apply to any "controller" or "processor" that conducts business in the state of Utah or which produces a product or service that is targeted to the residents of Utah and either (1) controls or processes personal data of 100,000 or more consumers during a calendar year or (2) derives over 50% of gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers. It would not apply to government entities, tribes, and non-profit corporations.

"Controller" is defined as a person doing business in the state who determines the purposes for which and the means by which personal data is processed, regardless of whether the person makes the determination alone or with others. A "processor" is a person who processes personal data on behalf of a controller.

What types of information would it cover?

The Act would apply to "personal data," defined as any information that identifies or describes an identifiable individual or is reasonable capable of identifying or describing an identifiable individual. Personal data does not include deidentified data, anonymous data, or publicly available information. Specific types of information excluded from the bill include protected health information, patient identifying information, and information provided for use in a consumer report. The Act also creates a category of "sensitive data," which includes racial or ethnic origin, religious beliefs, biometric information, and immigration status.

What rights would it create?

The bill provides consumers with the right to:

- confirm whether the controller is processing personal data concerning the consumer;
- obtain information regarding the categories of personal data collected;
- correct inaccurate personal data;
- delete personal data that the consumer provided to the controller;
- obtain a copy of the personal data in a portable and readily-usable form; and
- opt out of the processing of the consumers personal data for purposes of targeted advertising, sale of personal data, or profiling in furtherance of decisions regarding enrollment in an educational institution, criminal justice, employment opportunities, health care services, or access to basic necessities.

What obligations would it impose?

Under the bill, the controller must limit data collection to that which is relevant and reasonably necessary to achieve the controller's purposes. Controllers would also be required to provide a clear and reasonably accessible privacy notice informing consumers of the categories of personal data processed, how their personal data is used, and the manner in which the consumer may exercise the right to opt out. Processors would be required to adhere to the controller's instructions.

The controller would also be required to maintain reasonable security practices to protect confidentiality and to conduct an annual data protection assessment to evaluate any reasonably foreseeable risk to consumers related to the processing and security of personal data and sensitive data. Notably, the assessment would be considered a "confidential and protected record" under the Utah Government Records Access and Management Act—the disclosure of which to the Attorney General (AG) or the Division of Consumer Protection (the Division), as provided for in the Act, would not constitute a waiver of the attorney-client privilege or work product protection.

How would it be enforced?

There is no private right of action under Act; the AG has exclusive authority for enforcement. The Division would be empowered to investigate consumer complaints related to the Act and to refer matters to the AG if the Division has reasonable cause to believe that substantial evidence of a violation exists. Upon referral from the Division and following a 30 period to cure noticed violations, the AG may initiate an enforcement action and seek actual damages to the consumer *and* up to $1,000.00 per affected consumer for each violation. Any funds collected would be directed to a Consumer Privacy Account, which would be used for investigation and administrative costs, as well as enforcement and education activities.

Where does it stand?

Just last year, Utah Senate Bill 249 (the Utah Consumer Privacy Act) was defeated. Now, the Utah State Senate will again consider whether to pass a comprehensive consumer privacy bill. If enacted, the Utah Consumer Privacy Act would take effect on January 1, 2022.

Related Capabilities

Data Privacy, AI & Cybersecurity