New Year, New Data Privacy Laws in Multiple States

Jan 06, 2020

Categories:

Publications

Technology Blog

Businesses have more than the California Consumer Privacy Act (CCPA) to worry about in 2020 when it comes to privacy and data security regulations. In addition to the CCPA, other laws took effect on January 1 or will take effect later this year in states such as Maine, Oregon, and Connecticut. These data privacy laws are outlined below.

January 2020

California

California will begin to regulate the Internet of Things (IoT) by imposing additional security requirements on manufacturers of connected devices. SB 327 requires manufacturers of connected devices to equip them with reasonable security, including features that are:

- Appropriate to the nature and function of the device;
- Appropriate to the information the device collects, contains, or transmits; and
- Designed to protect the device and any information it contains from unauthorized, access, destruction, use, modification, or disclosure.

Also in California, the Social Media DISCLOSE Act would place additional restrictions on online platforms when related to political advertisements, such as:

- Displaying a "Who promoted this ad" link, disclosing who paid for certain political advertisements; and
- Maintaining a public record of political advertisements purchased and displayed in the last 12 months.

Illinois

The Artificial Intelligence Video Interview Act (HB2557) requires employers who use artificial intelligence (AI) to comply with multiple requirements before recording applicants and analyzing their

FBT Gibbons

characteristics through artificial intelligence. The law requires employers to:

- Notify each applicant before a video interview that AI may be used to analyze the video for consideration of the applicant for the position.
- Explain how the AI works and what general types of characteristics it uses to evaluate applicants;
- Obtain consent from the applicant prior to recording;
- Only share video with persons whose expertise or technology is necessary to evaluate the applicant's fitness for a position; and
- Upon request from an applicant, delete all copies of the applicant's video interview, including backup copies, within 30 days of the request.

Texas

HB 4390 amends the Texas Identity Theft Enforcement and Protection Act and requires:

- Creation of the Texas Privacy Protection Advisory Council "to study data privacy laws in this state, other states, and relevant foreign jurisdictions";
- Notification to individuals within 60 days if they are affected by a data breach; and
- Notification to the Texas attorney general within 60 days if personal information of more than 250 residents has been breached.

Oregon

The Oregon Consumer Information Protection Act, through SB 684, amends ORS 646A.600 – 646A0628 and requires:

- Vendors to separately notify the Oregon attorney general about a data breach; and
- Covered entities and vendors to develop, implement, and maintain reasonable safeguards to protect personal

information.

Oregon also amended ORS 646.607, which now requires manufacturers of connected devices to equip such devices with reasonable security features, such as:

- A means of authentication from outside a local area network, including a preprogrammed password that is unique to each connected device.

New Hampshire

SB 194 is New Hampshire's adoption of the NAIC Insurance Data Security Model Law. It requires qualifying insurance companies to:

- Develop, implement, and maintain a written information security program based on regular risk assessments.

March 2020

Washington

HB 1071 amends the state breach notification law by:

- Requiring businesses to disclose in their notifications the time frame of exposure in addition to the date of breach and date of discovery.
- Expanding the definition of personal information.

New York

The Stop Hacks and Improve Electronic Data Security (SHIELD) Act, S5575B, expands the definition of breach in New York's data breach statute to include:

- Additional categories of personal information.
- Entities with private information about New York residents and not just entities conducting business in New York.

The SHIELD Act calls for additional secuirty safeguards, including:

- Establishing and implementing a security training program;

- Assigning and designating employees to implement a security program;
- Identifying reasonably foreseeable internal and external risks;
- Disposing of private information after a reasonable time; and
- Selecting service providers capable of maintaining appropriate safeguards and requiring those safeguards on contracts with service provider.

Finally, the Act will expand exemptions under the data breach law as well as extend the statute of limitation regarding violations from two to three years.

October 2020

Connecticut

Connecticut, like New Hampshire, also adopted the NAIC Insurance Data Security Model Law by enacting its own version (HB-7474) requiring insurance companies to:

- Maintain an information security program proportionate to the size, nature, and complexity of their organizations;
- Perform regular risk assessments;
- Designate someone to be responsible for their information security program;
- Provide annual written certifications of compliance to the Connecticut Insurance Department; and
- Require their third-party service providers who control nonpublic information to implement appropriate security measures by October 2021.

Maine

In Maine, the Broadband Internet Access Service Customer Privacy Act prohibits using, selling, or distributing consumer data without consent and requires clear notice at the point of sale of the customer's rights and the provider's obligations.

For more information, please contact any attorney on Frost Brown Todd's Privacy & Data Security team.

FBT Gibbons