Hashed & Salted | A Privacy and Data Security Update
February 2022

State-Proposed Comprehensive Privacy Legislation in 2022

State legislatures across the United States wasted no time in 2022 introducing what they hope will be the next state-enacted comprehensive privacy law. In just the first three weeks of 2022, at least 27 comprehensive privacy bills were introduced in 16 states. We expect this trend to continue for the next several weeks and months. Many of the bills are similar to laws we have seen before, including the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), Virginia Consumer Data Protection Act (VCDPA) and Colorado Privacy Act (CPA). At the same time, each newly proposed bill includes its own nuances and specifications, which would make a "one size fits all" approach to privacy compliance in the United States nearly impossible. Moreover, in Massachusetts and New York, bills were carried over from the 2021 legislative session that would significantly expand models we have seen before. For example, these bills would require controllers to undertake the duties of care and loyalty to consumers. They would also restrict the permitted purposes for processing and require opt-in consent.

Discussed below are some of the key similarities and differences across proposed comprehensive privacy legislation introduced in Alaska, Florida, Kentucky, Indiana, Maryland, Massachusetts, Minnesota, Mississippi, Nebraska, New Jersey, New York, North Carolina, Ohio, Oklahoma, Pennsylvania and Washington. This includes a look at several of the bills that provide for a private right of action. We also take a deeper dive into the outliers introduced in Massachusetts, Nebraska and New York.

Similarities and Differences

A. Consumer Rights

Each bill provides some compilation of the following rights: access, deletion, correction, portability, objection to processing, restriction of processing, an opt-out of "selling," "targeted advertising" and/or certain kinds of sharing or an opt-in for certain kinds of processing and sharing, and the choice to either opt out or in for processing sensitive data.

B. Methods for Submitting Consumer Rights Requests

Several of the bills require one or more of three methods—toll-free number, email address and a web form—to allow consumers to submit requests. Under Alaska HB159/SB116, businesses would need to provide all three methods.

Attorney Advertising

Several bills provide consumers the right to opt out of "sale" or similar consumer rights via a link on the business homepage—something made popular by the CCPA. The links that some bills require include the following:

- Alaska HB159: "Do Not Collect or Sell My Personal Information"
- Alaska HB222: "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information"
- Florida HB9: "Do Not Sell or Share My Personal Information"
- Florida SB1864: "Do Not Advertise to Me" and "Do Not Sell My Personal Information"
- Mississippi SB2330: "Do Not Sell My Personal Information"
- New Jersey A332: (An unspecified opt-out link is required.)
- New York A3709/S567: "Do Not Sell My Personal Information"

C. User-Enabled Privacy Controls

Several of the bills require businesses to honor user-enabled privacy controls such as browser plug-ins or privacy settings, device settings, or other mechanisms to communicate or signal the consumer's choice to opt out of third-party trackers used to target advertising. These bills include the following:

- Florida HB9 (Honoring these controls is optional.)
- Florida SB1864
- New York A680b/S6701
- Washington HB1850

A working draft with the Alaska House Labor and Commerce Committee for HB159/SB116 would also require businesses to honor user-enabled privacy controls. In Washington state, Sen. Reuven Carlyle, in addition to reintroducing the proposed Washington Privacy Act, introduced SB5813, which would require businesses to honor Do Not Track (DNT) signals as valid requests to opt out of targeted advertising and the sale of personal data beginning July 1, 2024.

E. Private Right of Action

The following bills have a private right of action that is limited to data breaches:

- Alaska HB159/SB116
- Alaska HB222 (with a 30-day cure period)
- Mississippi SB2300 (with a 30-day cure period if curable)

The following bills have a private right of action that is limited to certain violations:

- Florida HB9 – The private right of action is for (i) failure to comply with consumer deletion, correction and opt-out requests and (ii) selling or sharing personal information of people under 17 without consent.
- Kentucky SB15 – The private right of action is for (i) failure to comply with consumer access, correction, deletion and opt-out requests; (ii) unlawful discriminatory data processing; and (iii) unlawful use of children's data. The court may award reasonable attorneys fees to prevailing plaintiffs.
- New York A680b/S6701 – The private right of action is for (i) failure to obtain opt-in consent for processing, (ii) failure to comply with automated decision-making obligations and (iii) failure to comply with consumer requests. The court may award reasonable attorneys' fees to a prevailing plaintiff.
- Washington SB5813 – The private right of action is for (i) failure to comply with a child's (under 13) or adolescent's (under 18) request to know, correct or delete; (ii) a data broker's failure to comply with a consumer request to know, correct or delete; and (iii) failure to honor a DNT signal. Remedies are limited to appropriate injunctive relief necessary and proportionate to remedy the violation. The court would also be required to award attorneys' fees to a prevailing plaintiff.

The following bills have a private right of action for any violation of the bill:

- Massachusetts S46 – The private right of action makes available liquidated damages in an amount not less than 0.15% of the annual global revenue of the covered entity or $15,000 per violation, whichever is greater; punitive damages; and any other relief the court deems appropriate. The court must award reasonable attorneys' fees and costs to any prevailing plaintiff.
- New York A3709/S567 – The private right of action is for statutory damages, and the plaintiff does not need to suffer a loss of money or property. In addition, anyone with nonpublic information may bring suit if they have knowledge of a violation. The person must first notify the attorney general and permit the attorney general to complete an investigation. If the attorney

general later prevails in court, the person who brought the violation to the attorney general's attention is awarded 15% of the civil penalties. If the person later brings suit and prevails, the court may award the person what the court deems reasonable between 25% and 50% of the civil penalties.

- North Carolina S569 – The private right of action may be brought by any injured person or deceased person's estate. The injured person may seek to enjoin and restrain future acts that would constitute a violation of the act. The court may award reasonable attorneys' fees to the prevailing party.
- New York A6042 – The private right of action provides for actual damages or liquidated damages of $10,000, whichever is greater; punitive damages; and other relief the court deems appropriate. The court must award reasonable attorneys' fees to the prevailing plaintiff.
- Washington HB1850 – The private right of action is for injunctive relief and actual damages. It includes a 30-day cure period.
- Washington HB1433 – This private right of action is up to $10,000 per violation and per individual or actual damages if greater. The court must award reasonable attorneys' fees and costs to any prevailing plaintiff.

F. Security

The majority of bills require controllers, processors and third parties to implement and maintain reasonable security measures. Only the Ohio Personal Privacy Act includes an enforcement safe harbor for adherence to the NIST Privacy Framework.

The Outliers

A. Massachusetts

The Massachusetts Information Privacy Act (MIPA) (S46) was originally introduced by state Sen. Cynthia Stone Creem in 2021. MIPA is one of the most comprehensive bills currently being considered. It requires opt-in consent for the processing of personal information, including personal information obtained from third parties. If a covered entity changes the nature of processing consented to, the covered entity must obtain consent for the changes two weeks prior to those changes taking effect. Once a year, covered entities would have to provide notice explaining how the personal information was used, including two examples of such use. A covered entity would not be permitted to de-identify an individual's personal information during the 60 days after the covered entity received a request for correction or deletion from that individual.

Covered entities would need to provide privacy policies in both long form and short form (no more than 600 words) that can be comprehended at the 8th grade reading level. The short-form privacy policy must include, among other things, one example of harm that may arise from the misuse of personal information.

MIPA regulates automated decision-making and imposes duties of care, loyalty and confidentiality. Further, these duties must be pushed down to any third-party recipient. Covered entities must take reasonable steps to ensure that third parties comply with these duties and obligations. A covered entity must inform the MIPA-created Massachusetts Information Privacy Commission if a data processor or a third party violates the MIPA.

B. Nebraska

Nebraska's bill, introduced on Jan. 20, 2002, would adopt the Uniform Personal Data Protection Act (UPDPA) (LB1188) drafted by the Uniform Law Commission.

Of interest, a controller may use personal data or disclose pseudonymized data to a third-party controller to deliver to a data subject targeted advertising and other purely expressive content. Privacy policies must include the federal, state or international privacy laws or frameworks with which the controller complies.

Processors must provide controllers with access to personal data, correct personal data, limit the use to that requested by the controller, conduct privacy and security assessments, and provide redress for prohibited data practices. The fact that a controller or processor conducted an assessment, the records analyzed in the assessment and the date of the assessment are not confidential under UPDPA.

A controller or processor is deemed to comply with the UPDPA if it complies with a comparable law protecting personal data in another jurisdiction and the attorney general determines the law in the other jurisdiction is at least as protective of personal data as the UPDPA. There is no private right of action.

C. New York

The New York Privacy Act (NYPA) (A680b/S6701) was reintroduced on Jan. 6, 2022. NYPA provides for a duty of loyalty and care and the right to access, delete, correct, restrict processing and portability. It requires notice and opt-in consent for processing and sharing with third parties. The notice must include the identity of the third party and the processing purposes for which the third party may use the personal data. The privacy notice must be at an eighth-grade reading level and include each third party with which the personal data was shared. If a controller is engaged in targeted advertising, the privacy notice must include the average expected revenue per user (ARPU) or a similar metric for the most recent fiscal year for the region that covers New York. Each version of the privacy notice from the previous six years must be accessible to consumers. The NYPA requires the disclosure of automated decision-making if used for certain decisions (e.g., housing and employment). Consumers must be provided with the ability to appeal the automated decision. Controllers must have a third-party, independent impact assessment conducted annually regarding its automated decision-making.

Conclusion

Each of these bills present similar but different enough approaches to privacy that compliance would need to be tailored for each state. As they work their way through the legislative process it is unlikely that all of the bills will survive. The next few months should provide more information about which bills are likely to pass into law. We will continue to monitor and provide updates on any significant developments.

Related Professionals

Tanya Forsheit . . . . . tforsheit@loeb.com
Jessica B. Lee . . . . . jblee@loeb.com
Shely Berry . . . . . sberry@loeb.com

6867 REV1 02-15-2022