MARCH 18, 2024

Spring 2024 – What Privacy Professionals Need to Know and Do Now in the U.S. – Part III

This year is proving to be just as an important year for privacy professionals as 2023. In our third installment of what privacy pros should know, we provide you with some highlights about the following important developments in U.S. privacy law:

- New Hampshire's recently enacted comprehensive privacy law
- The advancement of Kentucky's comprehensive privacy law to signature by the Governor
- A status update on Georgia's proposed comprehensive privacy law
- Information on how to comply with Washington's My Health My Data Act, parts of which come into effect on March 31, 2024.

Stay tuned for more information as we keep you updated with the latest trends in privacy.

New Hampshire Governor Signs Privacy Law

On March 6, Governor Sununu signed SB 255 (the "Act"), New Hampshire's comprehensive state privacy law, making it the 14th state to enact consumer privacy protections. New Hampshire's law is largely modeled after Virginia and other existing state laws, so compliance with the Act should lessen compliance obligations except with respect to responding to individual consumer requests in separate states.

The Act applies to individuals and business that conduct business in New Hampshire, or that produce products or services that are targeted to New Hampshire residents, that, during a one year period, controlled or processed the personal data of at least

1. 35,000 New Hampshire consumers (excluding data processed solely for the purpose of completing a payment transaction); or
2. 10,000 New Hampshire consumers and derives over 25% of their gross revenue from the sale of personal data.

The Act notably does *not* include a revenue threshold.

"Personal data", as defined by the Act, includes information that is linked or reasonably linkable to an identified or identifiable individual. De-identified data or publicly available information is not personal data under the law. This language closely follows the language under the Virginia Consumer Data Privacy Act.

The Act includes many similarly present exemptions in other state comprehensive privacy laws, including exemptions for government entities, nonprofits, higher education institutions, financial institutions, and covered entities and business associates under HIPAA.

The Act provides consumers with various rights regarding their data, including the right to confirm and access the personal data that a controller processes about them, correct inaccuracies in the data, delete, and port their data. In addition, businesses must provide consumers with an opportunity to opt out of the processing of their personal data for targeted advertising, the sale of their data, or automated decision-making profiling.

Controllers are required to respond to consumer requests no later than 45 days after receipt of the request.

Similar to other state privacy laws, controllers are obligated to comply with a number of requirements, including the following:

- Limit the collection of data to what is "adequate, relevant and reasonably necessary in reasonably necessary in relation to the purpose" for which data is processed (as disclosed to customers);
- Establish, implement, and maintain reasonable data security practices to protect personal data;
- Not process "sensitive data" (including information about race or ethnicity, religion, health conditions, sex life or orientation, citizenship or immigration status, genetic or biometric data, children's data, and precise geolocation data) without a person's consent; and
- Provide an effective mechanism for a consumer to revoke consent to processing their data.

Additionally, the Act restricts the ability to target advertising for children and sell the data of children between the ages of 13 – 16.

Processors must adhere to the controller's instructions and assist the controller in meeting the controller's obligations under the Act. Processors must also provide any necessary information to enable the controller to conduct and document data protection assessments, cooperate with data subject rights requests, and assist data controllers in meeting information security obligations.

The New Hampshire privacy law does not offer a private right of action. The Attorney General (AG) has the exclusive authority to enforce violations of the Act. The law provides for an enforcement grace period following enactment. Starting on January 1, 2025 and ending on December 31, 2025, the Attorney General must provide businesses with a notice of alleged violations and provide them with a 60-day period to cure any such violation before the AG can bring an enforcement action.

Kentucky's Privacy Proposal Moves Forward to the Governor

It's likely that Kentucky will soon be joining a growing number of states with comprehensive data privacy laws. As of March 11, 2024, Kentucky's SB 15 (the "Act") passed both the House and Senate of the Kentucky legislature, with a recent vote of 35-0 on two minor Floor Amendments in the Senate. The bill heads to the Governor's desk for signature, where it will become the 15 th U.S. state privacy law. If passed, Kentucky's privacy law would go into effect on January 1, 2026.

Kentucky's Act would apply to business entities that conduct business in the state or produce products or services in the state that target Kentucky residents, and that, during a calendar year, control or process personal data of at least:

1. 100,000 residents; or
2. 25,000 residents and derive over 50% of gross revenue from the sale of personal data.

The second applicability threshold is a unique provision to Kentucky's bill that means smaller businesses who rely heavily on data sales will be subject to the Act. Notably, the definition of "sale" is limited to an "exchange of personal data for monetary consideration."

The law exempts similar organizations as other state laws, including state entities; financial institutions subject to GLBA; HIPAA covered entities; nonprofits; institutions of higher education; as well as organizations that process data solely for the purpose of assisting law enforcement agencies in the pursuit of investigating insurance-related criminal or fraudulent acts or first responders; and small telephone or municipally owned utilities that do not sell or share personal data with third party processors. "Sharing" under the Act is defined as "disclosing personal data by a controller to a third party for targeted advertising or tracking, whether or not for monetary or other valuable consideration, including transaction […] in which no money is exchanged."

Under the Act, businesses are required to provide consumers with the rights to confirm whether their data has been processed; delete their data; correct inaccuracies in their data; port their data; and opt-out of targeted advertisements, profiling, and the sale of their data. Kentucky's Act requires controllers to recognize opt out requests made by consumers via "global privacy controls" or other browser or device settings.

Some other notable provisions of the law include prohibitions on controllers from processing sensitive data without allowing the consumer to opt out of such processing; processing the personal data of a child for the purposes of targeted advertising or tracking; and processing for the purposes of targeted advertising and tracking, selling, or sharing the personal data of consumers between the ages of 13 and 17 without their consent.

Kentucky's Act does not create a private right of action, but instead grants exclusive enforcement authority to the Kentucky Attorney General (AG). The AG is required to provide a 30-day cure period before initiating an enforcement action. The AG may seek damages for each violation for up to $7,500. The proceeds from the civil penalties imposed under the Act shall be held in a "consumer privacy fund," the details of the funds of which shall be used to "enforce the provisions" of the Act.

Privacy in the Peach State

In other state privacy news, on February 27, 2024, Senate Bill (SB) 473 to enact the Georgia Consumer Privacy Protection Act passed the State Senate. It is currently pending in the House Technology and Infrastructure Innovation Committee. The bill, as currently drafted, presents a number of common provisions that we have seen in other state comprehensive privacy laws. However, some notable items include the lack of data and entity-level exemptions found in other laws. Other provisions include:

- High applicability thresholds: The law applies to persons that conduct business in the state by producing products and services targeted to Georgia consumers that have revenue in excess of $25 million, and (a) control or process personal information of at least 25,000 consumers and derives more than 50% of their gross revenue from the sale of such information, or (b) control or process the personal information of at least 175,000 consumers in a calendar year.
- Consumer Rights: The law provides consumers with the right to access, correct, delete, port, and opt out of the processing of their personal information for the purposes of selling, profiling and targeted advertising.

- Penalties: Courts may impose a civil penalty of $7,500 for each violation of this law.
- Cure period: The Attorney General must provide controllers or processors 60 days' written notice and an opportunity to cure before initiating an action under the law.

Georgia's legislative session concludes on March 28, 2024, so time is running out for Georgia to pass this law.

Upcoming Deadline for Compliance with Washington's MHMDA

Companies that haven't yet examined if they're subject to Washington's My Health My Data Act (MHMD) should do so immediately. The law takes an extremely broad and unconventional view of what counts as health data (e.g., keystrokes, images, voices recordings, and precise geolocation). The law imposes substantial obligations and restrictions on entities involved in the collection, processing, sharing, and/or selling of consumer health data of Washington residents. Unlike most comprehensive consumer privacy laws, MHMD allows private plaintiffs to bring actions against companies for violations of the law, in addition to state attorney general enforcement.

Companies don't have much time between now and MHMD's effective date. Beginning as soon as March 31, 2024, regulated entities must comply with the Act's provisions, while small businesses are given until June 30, 2024.

The Washington Attorney General (AG) published a series of Frequently Asked Questions related to the My Health My Data Act, ostensibly to address some of the law's ambiguities. However, the AG has little incentive to offer the reprieve of helpful guidance through the FAQs (and wouldn't be beholden to such guidance in the event of an enforcement action anyways).

Nevertheless, the FAQs provide some sense of how the AG thinks about the law. Some of the key takeaways of the FAQs are:

- FAQ 3 states that out of state processors that process consumer health data for regulated entities or small business must comply with the Act (although in the role of a processor).
- FAQ 5 provides that consumer health data does not necessarily include information about a consumer's purchases that don't reveal a specific health condition, such as the purchase of toilet paper or deodorant. However, (1) information that identifies a consumer's past, present, or future physical or mental health status, and (2) information revealing a consumer's health status that is "derived or extrapolated" or inferred from non-health data (such as purchases) is considered consumer health data.

The AG noted that more FAQs may be forthcoming. We anticipate future updates as compliance dates pass and enforcement actions are brought. To be aware of what's expected for compliance in the coming days, some of the key provisions of the Act include:

- Burdensome consent requirements: Processing consumer health data must be based either on a consumer's consent, for security purposes, or as necessary to provide a service to consumers. Many uses of health data, e.g., advertising, cooperation with law enforcement, and product improvement, must be based on a consumer's consent. Regulated entities are thereby faced with a

choice of launching disruptive new consents or pulling Washington consumers' data from uses other than providing services to the consumer.

- Consumer health data privacy policy: Regulated entities and small businesses are required to publish and maintain a privacy policy that discloses: (1) the categories of consumer health data collected and the purpose for which the data is collected and used, (2) the categories of source from which the consumer health data is collected, (3) the categories of consumer health data that is shared, (4) a list of the categories of third parties, and specific affiliates, with whom the regulated entity or small business shares the consumer health data, and (5) how a consumer can exercise its rights.
- Valid data sale authorization: Before a business may sell or offer to sell consumer health data, it must obtain valid authorization from the consumer. The authorization is a distinct consent that needs to be obtained before the consumer's health data is collected and processed. The valid authorization must include a description of the purpose of the sale, a statement that the consumer can revoke the authorization, an expiration date of the valid authorization that expires a year from the date of the consumer's signature, and the signature of the consumer and the date. Purchasers and sellers of consumer health data are required to retain copies of valid authorizations for six years from the date of its signature.
- Restrictions on geofencing: The Act prohibits the placement and use of a geofence around an entity that provides in-person health services when the geofence is used for the purposes of identifying or tracking consumers seeking those services; collecting consumer health data from consumers; or sending notifications, messages, or ads to consumers related to their consumer health data or health care services.
- Private right of action: Washington residents may bring an action against a business for a violation of the Act under the Washington Consumer Protection Act, but technical violations of MHMD shouldn't be actionable. Fortunately for businesses, the law under which private plaintiffs must bring MHMD violations (the Washington Consumer Protection Act) requires plaintiffs to show an "injury" to business or property. Pure privacy harms don't necessarily give rise to such an injury.

As always, we are here to answer any questions you may have about the MHMDA and what it means for your company's operations.

We would also be remiss if we didn't mention that the EU's AI Act was passed on March 13, 2023. We expect this law to be as impactful to privacy pros as the GDPR was. For more information about the EU AI Act, you can read more by Kilpatrick's Jon Neiditz here.