WILMERHALE

State Comprehensive Privacy Law Update

March 8, 2023

Since our last update, comprehensive privacy law proposals have continued to emerge and progress through state legislatures. Most notably, five bills have now passed a legislative chamber, with Hawaii's Consumer Data Protection Act (SB 974), Iowa's SF 262, and Montana's Consumer Data Privacy Act (SB 384) joining the previously covered Indiana Senate Bill 5 and New Jersey S. 332.

Meanwhile, new bills continue to be proposed. Five new states (Rhode Island, Illinois, Montana, West Virginia, and Florida) have seen the introduction of comprehensive bills, bringing the total to 21 states thus far this legislative session. And a bill in one of those states — Montana's SB 384 — has already passed the state senate.

These developments take place as Congress moves to revisit a federal data privacy bill. On March 1, the House Committee on Energy and Commerce's Subcommittee on Innovation, Data, and Commerce held a hearing titled "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy." A key takeaway of this hearing is that Congress appears poised to resume efforts to pass some version of the American Data Privacy and Protection Act (ADPPA), a federal privacy proposal that was approved by the committee at the end of last year, but ultimately failed to progress any further in the legislative process. Notably, the ADPPA would have preempted many state comprehensive privacy laws — thus, should Congress pass similar legislation this year, it may have the effect of overriding any state comprehensive privacy laws on the books.

To keep updated on comprehensive privacy law developments at both the federal and state levels, be sure to subscribe to the WilmerHale Privacy and Cybersecurity Law Blog.

NEW PROPOSALS

Nine new comprehensive privacy bills have been proposed since our last update. Besides the six bills across Rhode Island, Illinois, Montana, West Virginia, and Florida (with two in West Virginia), other bills have been proposed in Kentucky, Minnesota, and New York. Of these nine bills, Montana's Consumer Data Privacy Act (SB 384) has already passed the state senate, while West

Virginia's HB 3498 has received committee approval. Further, the Illinois Data Privacy and Protection Act (HB 3385) will receive a committee hearing on March 9, demonstrating a possibility for advancement.

Notably, only three of the nine proposals — specifically, the Illinois Data Privacy and Protection Act (HB 3385), the New York Privacy Act (A3593), and West Virginia's HB 3453 — create private rights of actions. While the Illinois and New York bills broadly allow consumers to bring actions for any Act violation, the West Virginia private right of action is more limited, applying only to victims of specified data breaches. Additionally, seven out of the nine bills contain cure-period provisions providing covered entities the opportunity to avoid enforcement action if they remedy a violation within a specified time period (ranging from 30 to 60 days, depending on the bill).

Florida

1. *Bill Title:* Senate Bill 262

2. *Current Status:* As of March 7, 2023, SB 262 has been referred to the Senate Commerce and Tourism Committee (3/6/23).

3. *Key Provisions:*

- Applies to entities that are organized or operated for the profit or financial benefit of shareholders, do business in the state, collect consumer personal information and determine the purpose for such collection, have a gross revenue in excess of $1 billion, and satisfies one of the following: (1) derive 50% or more of gross revenue from providing targeted advertising or the sale of ads or (2) operate a consumer smart speaker or voice command component connected to a cloud.
- Exempts various entities and information types, including entities and information subject to HIPAA, entities subject to GLBA, information subject to FCRA, information subject to FERPA, information collected for the purpose of payment transactions, deidentified personal information or aggregated consumer information, and certain employment related information.
- Prohibits government entities and employees of such entities from communicating with social media platforms to request the removal of content or accounts from such social media platform, or for the purpose of content moderation. Provides exceptions for certain circumstances, such as where public safety is implicated.
- Affirms individual rights granted to consumers, including the right to know the types of information a controller collects, the consumer's right to request the deletion or correction of inaccurate data, and the consumer's right to opt out of the sale or sharing of their personal information with third parties.

- Requires that controllers obtain consent before processing sensitive data, such as geolocation data.
- Requires that a controller disclose how algorithms are used on a search engine to prioritize and deprioritize political partisanship or political ideology in search results.
- Does not create a private right of action. State AG has exclusive authority to enforce Act.
- The state AG can seek civil penalties of up to $50,000 per violation. Civil penalties can be tripled where the covered entity: (1) processes a child's (18 years or younger) information in violation; (2) fails to process a consumer's request to delete or correct; (3) fails to comply with the consumer's request to opt-out of sharing with third parties.
- Allows the state AG discretion to grant a 45-day cure period for entities alleged to have violated the Act.
- Would go into effect on July 1, 2023.

Illinois

1. *Bill Title:* Illinois Data Privacy and Protection Act (HB 3385)

2. *Current Status:* As of March 7, 2023, the bill will receive a hearing before the House Cybersecurity, Data Analytics, and IT Committee on March 9 (2/28/23).

3. *Key Provisions:*

- Generally applies to "covered entities," which includes any non-government entity that "determines the purposes and means of collecting, processing, or transferring covered data."
- Limits covered entities to data collection and processing that is "reasonably necessary and proportionate" to (1) "provide or maintain a specific product or service requested by the individual to whom the data pertains"; or (2) effect one of a series of enumerated purposes (e.g., authentication, compliance with legal obligation, fulfill warranty).
- Imposes a duty of loyalty on covered entities, including limitations on their collection and processing of Social Security numbers and sensitive covered data.
- Incorporates privacy by design principles, including mitigation of privacy risks throughout the product development lifecycle and implementation of reasonable training and safeguards to ensure compliance with relevant privacy laws.
- Creates individual rights for consumers, including the right to access personal data collected by a covered entity, as well as additional information about data transferred to

third parties; the right to correct personal data; the right to delete personal data; and the right to obtain a portable copy of personal data.

- Requires that covered entities obtain individual consent before transferring personal data to a third party or delivering targeted advertising.
- Requires that covered entities implement reasonable data security practices, including risk and vulnerability assessment, disposal of data pursuant to an established retention schedule, employee training, and incident detection and response.
- Requires that large data holders make annual compliance certifications to the state AG.
- Requires covered entities (excluding small businesses) to appoint at least one privacy officer and at least one data security officer. Large data holders further required to appoint a privacy protection officer responsible for developing and implementing audit, training, and policy review procedures.
- Requires that covered entities (excluding small businesses) perform biennial privacy impact assessments covering all data processing activities that "may cause a substantial privacy risk."
- Authorizes state AG, State's Attorney, and municipality attorneys to bring civil actions to enforce Act (including damages, civil penalties, and other compensation).
- Creates private right of action for individuals who suffer violation of Act. Plaintiffs may obtain damages, injunctive relief, and declaratory relief. Private right of action does not apply to claims against small businesses.
- Authorizes state AG to adopt rules to implement Act.
- Act would take effect 180 days after enactment.

Kentucky

1. *Bill Title:* House Bill 301

2. *Current Status:* As of March 7, 2023, HB 301 had been referred to the House Small Business and Information Technology Committee (2/17/23).

3. *Key Provisions:*

- Applies to entities that conduct business in Kentucky or produce services or products targeted to Kentucky residents and during a calendar year control or process personal data of at least: (a) 100,000 consumers; or (b) 25,000 consumers and derive more than 50% of gross revenue from sale of personal data.

- Exempts various entities and information types, including state political or judicial entities, nonprofit organizations, institutions of higher education, entities and information subject to HIPAA, entities subject to GLBA, information subject to FCRA, information subject to FERPA, and certain employment-related information. In addition, an entity that complies with COPPA's parental consent requirements is deemed compliant with the Act's parental consent requirements.
- Creates individual rights for consumers, including the right to confirm whether a controller is processing personal data; the right to access personal data; the right to delete data; the right to obtain a portable copy of personal data; and the right to opt out of the processing of data for purposes of targeted advertising and sale of data.
- Incorporates privacy by design principles, including purpose limitation and reasonable security measures.
- Requires that controllers obtain consumer consent before processing sensitive data, which includes biometric data.
- Requires that controllers provide meaningful notice which includes providing consumers with a description of the categories of personal information being processed; purpose for processing; categories of data shared with third parties and which third parties receive shared information; and a disclosure of targeted advertising practices.
- Does not create a private right of action. State AG has exclusive authority to enforce Act.
- Creates a 30-day cure period for violators before the state AG may bring an enforcement action.
- Imposes civil penalties of up to $7,500 per violation. All civil penalties collected will be used to fund the "Consumer Privacy Fund" used to fund future enforcement actions.
- Would go into effect on January 1, 2025.

Minnesota

1. *Bill Title:* Minnesota Consumer Data Privacy Act (HF 2309)

2. *Current Status:* As of March 7, 2023, HF 2309 had been referred to the House Commerce Finance and Policy Committee (3/1/23).

3. *Key Provisions:*

- Applies to entities that conduct business in Minnesota or produce services or products targeted to Minnesota residents and during a calendar year control or process personal data of at least: (a) 100,000 consumers; or (b) 25,000 consumers and derive more than 25% of gross revenue from sale of personal data.

- Exempts various entities and information types, including government entities; federally recognized Indian tribes; entities and information subject to HIPAA; entities subject to GLBA; information subject to FCRA, FERPA, and the Minnesota Insurance Fair Information Reporting Act; and certain employment-related information. In addition, an entity that complies with COPPA's parental consent requirements is deemed compliant with the Act's parental consent requirements. Although the Act does not provide exemptions for nonprofits or higher education institutions, the Act will not apply to these entities until July 31, 2028.
- Creates individual rights for consumers, including the right to confirm whether a controller is processing personal data; the right to access personal data; the right to correct data; the right to delete data; the right to obtain a portable copy of personal data; and the right to opt out of the processing of data for purposes of targeted advertising, sale of data, and "profiling in furtherance of solely automated decisions that produce legal or similarly significant effects." It also creates a right for consumers to question and receive explanation of the results of such profiling where profiling is used to make a decision regarding the consumer.
- Requires a controller to process consumer opt-out requests provided via universal opt-out mechanisms.
- Requires that controllers provide meaningful notice which includes providing consumers with a description of the categories of personal information being processed; the collection source for such data; purpose for processing; categories of data shared with third parties and which third parties receive shared information; a disclosure of targeted advertising practices; among other disclosures.
- Incorporates privacy by design principles, including purpose limitation and reasonable security measures.
- Requires that controllers obtain consumer consent before processing sensitive data, which includes biometric data.
- Requires controller to conduct data protection assessment for processing activities that "present a heightened risk of harm to a consumer," including processing for purposes of targeted advertising, sale of personal data, and processing for purposes of profiling (where profiling presents certain specified risks).
- Does not create a private right of action. State AG has exclusive authority to enforce Act.
- Creates a 30-day cure period for violators before the state AG may bring an enforcement action, which would expire on January 31, 2026.
- Imposes civil penalties of up to $7,500 per violation.
- Would go into effect on July 31, 2024.

Montana

1. *Bill Title:* Consumer Data Privacy Act (SB 384)

2. *Current Status:* As of March 7, 2023, the bill had been passed by the Senate and transmitted to the House (3/3/23).

3. *Key Provisions:*

- Applies to entities that conduct business in Montana or produce services or products targeted to Montana residents and control or process personal data of not less than: (1) 100,000 consumers, excluding personal data processed for the purpose of payments; or (2) 25,000 consumers and derive more than 25% of gross revenue from sale of personal data.
- Exempts various entities and information types, including state political or judicial entities, nonprofit organizations, institutions of higher education, specified national securities associations, entities and information subject to HIPAA, entities subject to GLBA, information subject to FCRA, information subject to FERPA, information governed by the Driver's Privacy Protection Act, information governed by the Farm Credit Act, and certain employment-related information. In addition, an entity that complies with COPPA's parental consent requirements is deemed compliant with the Act's parental consent requirements.
- Creates individual rights for consumers, including the right to confirm whether a controller is processing personal data; the right to access personal data; the right to correct data; the right to delete data; the right to obtain a portable copy of personal data; and the right to opt out of the processing of data for purposes of targeted advertising, sale of data, and "profiling in furtherance of solely automated decisions that produce legal or similarly significant effects."
- Incorporates privacy by design principles, including purpose limitation and reasonable security measures.
- Requires that controllers obtain consumer consent before processing sensitive data, which includes biometric data.
- Requires controller to conduct data protection assessment for processing activities that "present a heightened risk of harm to a consumer," including processing for purposes of targeted advertising, sale of personal data, and processing for purposes of profiling (where profiling presents certain specified risks).
- Does not create a private right of action. State AG has exclusive authority to enforce Act.
- Creates a 60-day cure period for violators before the state AG may bring an enforcement action.
- Act would be enforced under the Montana Unfair Trade Practices and Consumer Protection Act, which imposes civil penalties of up to $10,000 per violation. § MCA 30-14-142.

- Would go into effect on July 1, 2025, with certain sections taking effect on July 1, 2023.

New York

1. *Bill Title:* New York Privacy Act (A3593)

2. *Current Status:* As of March 7, 2023, A3593 has been referred to the Assembly Consumer Affairs and Protection Committee (2/3/23).

3. *Key Provisions:*

- Applies to entities that conduct business in New York or produce services or products targeted to New York residents that satisfy one or more of the following thresholds: (a) have annual gross revenue of 25 million dollars or more; (b) controls or processes personal data of 100,000 consumers or more; (c) controls or processes personal data of 500,000 natural persons or more nationwide, and controls or processes personal data of 10,000 consumers or more; or (d) derives over fifty percent of gross revenue from the sale of personal data, and controls or processes personal data of twenty-five thousand consumers or more.
- Exempts various entities and information types, including state political or judicial entities, specified national securities associations, entities and information subject to HIPAA, entities subject to GLBA, information subject to FCRA, information subject to FERPA, information governed by the Driver's Privacy Protection Act, information governed by the Farm Credit Act, certain employment-related information, and certain education related information. In addition, an entity that complies with COPPA's parental consent requirements is deemed compliant with the Act's parental consent requirements.
- Requires that controllers provide meaningful notice which includes providing consumers with a description of the categories of personal information being processed; the collection source for such data; purpose for processing; categories of data shared with third parties and which third parties receive shared information; a disclosure of targeted advertising practices; among other disclosures. This notice must be updated annually.
- Requires unambiguous opt-in consent for the collection of personal information, as well as upon changes in the purpose or type of collection.
- Creates individual rights for consumers, including the right to confirm whether a controller is processing personal data; the right to access personal data; the right to correct data; the right to delete data; and the right to obtain a portable copy of personal data.
- Creates additional rights for consumers when controller uses automated decision making in certain situations, such as for the denial of financial or lending services, housing, and public accommodation, among others.

- Requires controller to conduct data protection assessment for processing activities that "present a heightened risk of harm to a consumer," including processing for purposes of targeted advertising, sale of personal data, and processing for purposes of profiling (where profiling presents certain specified risks).
- Incorporates privacy by design principles, including purpose limitation and reasonable security measures.
- Requires data brokers to register, pay an annual fee to the New York AG, and submit information regarding their data use practices, including a description of the method of processing consumer requests.
- Creates a private right of action. A court may award plaintiffs actual damages or $1,000, whichever is greater.
- Violations are also enforceable by the New York AG who may seek civil penalties of up to $15,000 per violation.
- Most provisions would take effect two years after enactment, while the private right of action will take effect three years after enactment.

Rhode Island

1. *Bill Title:* Rhode Island Personal Data and Online Privacy Protection Act (H5745)

2. *Current Status:* As of March 7, 2023, the House Innovation, Internet, and Technology Committee had held the bill for further study (3/2/23). (This means that the bill is unlikely to advance further).

3. *Key Provisions:*

- Applies to entities that conduct business in Rhode Island or produce products or services targeted to Rhode Island residents and that, during the preceding calendar year, satisfied one of the following requirements: (1) controlled or processed personal data of at least 100,000 consumers; or (2) controlled or processed personal data of at least 25,000 consumers and derived more than 25% of gross revenue from sale of personal data.
- Exempts state government (and subdivision) entities, nonprofits, higher-education institutions, entities and information subject to GLBA, entities and information subject to HIPAA, information governed by FCRA, information governed by FERPA, and certain employment-related information. In addition, entities that comply with COPPA's parental consent requirements are deemed compliant with the Act's parental consent requirements.
- Creates individual rights for consumers, including: the right to confirm whether a controller is processing personal data; the right to access personal data processed by a controller;

the right to correct personal data; the right to delete personal data; the right to obtain a portable copy of personal data; the right to opt out of the processing of personal data for purposes of targeted advertising, sale of personal data, and "[p]rofiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer."

- Allows consumers to exercise their opt-out rights via browser settings, browser extensions, global device settings, and opt-out preference signals. Controllers are required to have the capability to process opt-out preference signals by January 1, 2025.
- Incorporates privacy by design principles, such as purpose limitation and reasonable security measures.
- Requires that controllers obtain consumer consent before processing sensitive data.
- Requires that controllers conduct data protection assessments for processing activities that "present a heightened risk of harm to a consumer," including processing for purposes of targeted advertising, sale of personal data, processing for purposes of profiling (where profiling presents certain specified risks), and processing of sensitive data.
- Grants state AG exclusive authority to enforce the Act. Does not create a private right of action.
- Creates a 60-day cure period for violators before state AG may initiate civil action. Cure period provision expires on December 31, 2024. Beginning in 2025, state AG would have the discretion to allow violators to cure.
- Violations of the Act would constitute unfair sales and deceptive trade practices under Rhode Island state law.
- Requires the Rhode Island General Assembly to convene joint study commission to study, among other things, algorithmic decision-making, children's privacy, and data colocation.
- Act would take effect on July 1, 2023.

West Virginia

1. *Bill Title:* HB 3453

2. *Current Status:* As of March 7, 2023, the bill had been introduced and referred to the House Technology and Infrastructure Committee (2/14/23).

3. *Key Provisions:*

- Applies to businesses that do business in West Virginia, collect and "[d]etermine[] the purposes and means of processing" consumer personal information, and satisfy at least one of the following requirements: (1) global annual gross revenues exceeding $25

million; (2) annually buys, receives, sells, or shares personal information of 50,000 or more consumers, households, or devices; or (3) derives 50% or more of global annual revenues from selling or sharing consumer personal information.

- Creates individual rights for consumers, including the right to access personal data collected by a business (and additional information about that data, such as purposes for collection or sale and entities from/to which the data is collected or sold), the right to correct personal data, the right to delete personal data, the right to opt-out of the sale or sharing of personal data, the right to obtain a portable copy of personal data, and the right to request information about personal data sold or shared (e.g., categories of information sold or shared, categories of third parties to which personal data was sold or shared).
- Requires that businesses dispose of personal data upon the earliest of (1) the satisfaction of the purpose for collecting the data; (2) the end of the relevant contract; or (3) 1 year after the consumer's last interaction with the business.
- Requires that businesses post a "Do Not Sell or Share My Personal Information" link on their Internet homepages allowing consumers to exercise their right to opt-out.
- Creates a private cause of action for consumers whose "nonencrypted and nonredacted personal information or e-mail address, in combination with a password or security question and answer that would allow access to the account" is compromised as a result of a business's failure to implement reasonable security practices. Consumers may obtain the greater of $100–$750 per consumer per incident or actual damages.
- Authorizes West Virginia Division of Consumer Protection to bring actions against violating businesses. Division may seek civil penalty of no more than $2,500 per unintentional violation and $7,500 per intentional violation, with penalties tripled if the violation involved a consumer of 16 years of age or younger.
- Creates a 30-day cure period for violators before Division may bring enforcement action.
- Authorizes the Division of Consumer Protection to adopt rules to implement the Act.

West Virginia

1. *Bill Title:* HB 3453

2. *Current Status:* As of March 7, 2023, the bill had been passed by the Technology and Infrastructure Committee and referred to the Finance Committee (2/20/23).

3. *Key Provisions:*

- Applies to entities that conduct business in West Virginia or produce products or services targeted to West Virginia residents and, during a calendar year, satisfy at least one of the

following: (1) control or process personal data of at least 100,000 consumers; or (2) control or process personal data of at least 25,000 consumers and derive over 50% of gross revenue from sale of personal data.

- Exempts various entities and information types, including state and local government entities, financial institutions and data subject to GLBA, entities and information subject to HIPAA, nonprofit organizations, institutions of higher education, information subject to FCRA, information subject to FERPA, and certain employment-related information. In addition, entities that comply with COPPA's parental consent requirements are deemed to comply with the Act's parental consent requirements.
- Creates individual rights for consumers, including: the right to confirm whether a controller is processing personal data and to access said data; the right to correct personal data; the right to delete personal data; the right to obtain a portable copy of personal data; and the right to opt out of the processing of personal data for purposes of targeted advertising, sale of personal data, and "[p]rofiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer."
- Incorporates privacy by design principles, such as purpose limitation and reasonable security measures.
- Prohibits controller from processing sensitive data without individual's consent.
- Requires that controllers conduct data protection assessments for processing activities that "present a heightened risk of harm to consumers," including: processing of personal data for purposes of targeted advertising, sale of personal data, processing of data for purposes of profiling (where profiling presents certain specified risks), and processing of sensitive data.
- Grants state AG exclusive authority to enforce the Act. Does not create a private right of action. State AG may seek damages of up to $7,500 per violation.
- Creates a 30-day cure period for violators before state AG may initiate action.
- Requires that state AG set up process by which consumers may exercise the Act's consumer data privacy rights "through the agency of the Attorney General's Office."
- Establishes a Consumer Privacy Fund in the state treasury, into which civil penalties collected under the Act will be deposited.
- Act would become effective on January 1, 2024.

Updates on Existing Proposals

In addition to the previously discussed Montana SB 384, two additional bills passed a legislative chamber in the past few weeks. Hawaii's Consumer Data Protection Act (SB 974) passed the

Hawaii Senate on March 7, and Iowa's SF 262 passed the Iowa Senate the day before, on March 6. Notably, neither of these bills contains a private right of action.

These bills join Indiana Senate Bill 5 and New Jersey's S. 332 as the only comprehensive bills to have passed a chamber in the 2023 legislative session thus far. There has not been much progress on those two bills since our last update. Indiana Senate Bill 5 was referred to the House Judiciary Committee on February 28, while New Jersey S. 332 remains under consideration by the Assembly Science, Innovation, and Technology Committee.

Other bills continue to move forward in the legislative process as outlined below.

- **Committee Approvals:**
  - Iowa SF 262's companion bill, HF 346, was approved by the Committee on Economic Growth and Technology on February 15 and awaits consideration by the full House.
  - Kentucky Senate Bill 15 was approved by the Senate Economic Development, Tourism, and Labor Committee on February 23. It now resides with the Senate Rules Committee. Notably, while SB 15 is generally enforced by the state AG, it does create a limited private right of action for individuals alleging that a controller failed to comply with a consumer rights request.
  - Oklahoma's Computer Data Privacy Act (HB 1030) was passed by the House Government Modernization and Technology Committee on February 21. It now awaits consideration by the full chamber. Notably, HB 1030 would require that businesses obtain consent from consumers before they collect consumer personal information. The state AG would be the Act's sole enforcement mechanism.
- **Committee Hearings and Calendar Placements:**
  - New Hampshire's Senate Bill 255 received a hearing before the Senate Judiciary Committee on February 14.
  - Maryland's Online and Biometric Data Privacy Act received a hearing before the House Economic Matters Committee on February 22. The Act's Senate version will receive a hearing before the Senate Finance Committee on March 8.
  - Oregon's Senate Bill 619 received a hearing before the Judiciary Committee on March 7.
  - Tennessee's Information Protection Act (SB 73) has been placed on the Commerce and Labor Committee calendar for March 14.
- **New Companion Bills:**
  - Several bills that we have previously analyzed have new companion bills:
    - HB 4, a companion bill to the Texas Data Privacy and Security Act (HB 1844) was introduced on February 16 and referred to the House Business and

Industry Committee on February 23. Incidentally, HB 1844 was subsequently referred to the same committee on March 7.

- A companion bill to New York's Digital Fairness Act (S2277) was introduced in the Assembly (A3308) on February 2, where it has been referred to the Consumer Affairs and Protection Committee.
- A companion bill to New York's S3162 was introduced in the Assembly (A4374) on February 14 and has also been referred to the Consumer Affairs and Protection Committee.

Contributors

Kirk Nahra
PARTNER

kirk.nahra@wilmerhale.com
+1 202 663 6128

Ali Jessani
SENIOR ASSOCIATE

ali.jessani@wilmerhale.com
+1 202 663 6105

Genesis Ruano
ASSOCIATE

genesis.ruano@wilmerhale.com
+1 202 663 6154

Samuel Kane
ASSOCIATE

samuel.kane@wilmerhale.com
+1 202 663 6114