State Comprehensive Privacy Law Update – January 30, 2023

2023 continues to be a busy year for state comprehensive privacy legislation. Since our last post, several new states have entered the fray with legislative proposals, while some of the bills we previously examined have moved forward in the legislative process. To date, we have seen at least 13 states propose some form of comprehensive privacy legislation.

This post summarizes new bills proposed in Hawaii, Indiana, Massachusetts, New Hampshire, New York, Vermont, and Washington, as well as provides updates on several previously proposed bills that we are continuing to track. We have not yet seen a bill make significant traction through the legislature, but we will continue to keep you posted on updates to these bills and others as they occur.

NEW PROPOSALS

The These new bills generally align with the trends we observed in our last post, as well as the structure of those previous proposals. One exception is Massachusetts's Internet Bill of Rights (HD 3245), which features provisions largely modeled after the General Data Protection Regulation (GDPR) in the European Union. This is the first GDPR imitator that we have seen in this year's legislative sessions.

Hawaii

1. *Bill Title:* Consumer Data Protection Act (SB 974)
2. *Current Status:* As of January 29, 2023, the bill had been referred to the Committee on Commerce and Consumer Protection and the Committee on Ways and Means.
3. *Key Provisions:*

- Applies to entities that conduct business in Hawaii or produce products or services targeted to Hawaii residents and satisfy at least one of the following requirements: (1) control or process personal data of at least 100,000 consumers in a calendar year; or (2) control or process personal data of at least 25,000 consumers and derive over 25% of gross revenue from sale of personal data.

- Exempts various entities and information types, including government entities, nonprofit organizations, and higher-education institutions; information governed by HIPAA, GLBA, FCRA, and 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 processing of and access personal data; the right to correct inaccurate 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 data, and profiling in furtherance of certain types of decisions (e.g., financial, housing, criminal justice, health care).
- Allows consumers to exercise their opt-out rights through browser settings, browser extensions, and global device settings.
- Incorporates privacy by design principles, such as purpose limitation and reasonable security practices.
- Requires that controllers obtain consent before processing consumers' sensitive data.
- Requires that controllers conduct data protection assessments for processing activities including: processing of personal data for purposes of targeted advertising; sale of personal data; processing of personal data for purposes of profiling, where profiling presents certain "reasonably foreseeable risk[s]"; processing of sensitive data; and any processing that "present[s] a heightened risk of harm to consumers." This requirement applies only to processing activities generated after January 1, 2025.
- Grants state AG exclusive authority to enforce the Act. Does not create a private right of action.
- Creates a thirty-day cure period for violators before state AG may initiate a civil action.
- State AG may seek civil penalty of up to $7,500 per violation, as well as injunctive relief.
- Authorizes state AG to adopt rules to support implementation of the Act.
- Establishes a consumer privacy special fund, administered by the state AG, into which civil penalties and other assets collected under the Act will be deposited.
- Act would take effect on July 1, 2023.

Hawaii

1. *Bill Title:* Consumer Data Protection Act (SB 1110)
2. *Current Status:* As of January 29, 2023, the bill had been referred to the Committee on Commerce and Consumer Protection, the Committee on Judiciary, and the Committee on Ways and Means.
3. *Key Provisions:*

- Applies to entities that conduct business in Hawaii or produce products or services targeted to Hawaii residents and satisfy at least one of the following requirements: (1) control or process personal data of at least 100,000 consumers in a calendar year; 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 government entities, entities and data subject to GLBA, entities and data subject to HIPAA, nonprofit organizations, institutions of higher education, personal information subject to FCRA, personal data subject to FERPA, and certain employment-related data. 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 processing of and access personal 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 profiling "in furtherance of decisions … that produce legal or similar significant effects concerning the consumer."
- Incorporates privacy by design principles, such as purpose limitation and reasonable security practices.
- Requires that controller obtain consumer's consent before processing sensitive data.
- Requires that controllers conduct data protection assessments for processing activities including processing personal data for purposes of targeted advertising; sale of personal data; processing of personal data for purposes of profiling when profiling presents certain "reasonably foreseeable risk[s]"; processing of sensitive data; and any processing that "present[s] a heightened risk of harm to consumers." This requirement applies only to processing activities generated after January 1, 2024.
- Violations of Act would constitute "unfair method of competition and unfair and deceptive acts or practices" under Haw. Rev. Stat. § 480-2. Violations would be subject to a civil penalty of $500 to $10,000 per violation, pursuant to Haw. Rev. Stat. § 480-3.1. Under § 480-3.1, either the state AG or the Director of the Office of Consumer Protection could bring a civil action to collect this penalty.
- Creates private right of action for consumers injured by violation of Act, pursuant to Haw. Rev. Stat. § 480-2.
- Authorizes state AG to adopt rules to support implementation of the Act.
- Act would take effect on July 1, 2023.

Indiana

1. *Bill Title:* Consumer Data Protection (House Bill 1554)
2. *Current Status:* As of January 29, 2023, the bill had been referred to the Committee on Commerce, Small Business and Economic Development.
3. *Key Provisions:*

- Applies to businesses that conduct business in Indiana, produce products or services that are purchased or used by residents of Indiana, and during a calendar year control or process personal data of either: 1) at least 100,000 consumers; or 2) at least 25,000 consumers and derive more than fifty percent of gross revenue from the sale of personal data.

- Exempts various entities and information types, including state government entities; financial institutions and data subject to GLBA; covered entities, business associates, and protected health information governed by HIPAA; controller or processors that comply with COPPA; information governed by FCRA; information governed by the Driver’s Privacy Protection Act; personal data governed by FERPA; and personal data governed by the Farm Credit Act.
- Creates individual rights for consumers, including the right to confirm whether their data is being processed; the right to access their data; the right to correct inaccuracies; the right to delete data provided; the right to obtain a copy of the personal data they previously provided to the controller in a portable and readily usable format; and the right to opt out of processing for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similar effects concerning the consumer.
- Incorporates privacy by design principles, such as purpose limitation and reasonable security practices. Controllers are further prohibited from collecting additional categories of personal information or using collected information for additional purposes without obtaining consumer consent.
- Creates additional requirements for processing sensitive data.
- Requires controllers to conduct a data protection assessment for data processed after December 31, 2023.
- Requires that the Attorney General Division of Consumer Protection maintain and publish a “Do Not Sell List” that includes the email addresses of consumers who request that their personal data not be sold. Controllers are required to provide a “Do Not Sell My Personal Information” link on their internet homepages allowing consumers to exercise their right to opt out.
- Requires data brokers to register, pay an annual fee to the Indiana AG, and submit information regarding their data use practices, including a description of the method of processing consumer requests.
- Does not create a private right of action. Violations are only enforceable by the Indiana AG. Additionally, the Act provides the state AG with the option to create an online portal to facilitate receipt of consumer requests for controllers or processors, as well as adopt rules to enforce as necessary.
- Creates a thirty-day cure period after the state AG provides written notice. If entity cures violation and provides the state AG an express written statement, no action for statutory damages will be initiated. This provision expires January 1, 2026.
- Imposes civil penalties of up to $7,500 for each violation. The state AG may recover reasonable expenses incurred in investigating and preparing the case, including attorneys’ fees.
- Would go into effect on January 1, 2024.

Massachusetts

1. *Bill Title:* Massachusetts Information Privacy and Security Act (SD 1971/HD 3263)
2. *Current Status:* As of January 29, 2023, the bills had been filed on the Senate and House dockets.
3. *Key Provisions:*

- Applies to (1) controllers and processors that conduct business in Massachusetts; (2) processing of personal information by controllers and processors not established in Massachusetts, when processing is related to (a) offering of goods or services targeted to Massachusetts residents or (b) monitoring of Massachusetts residents' behavior when behavior takes place in Massachusetts; (3) entities that agree to be bound by the Act.
- Additionally, sections 7–17 and 26 (which primarily address consumer rights and the Act's private right of action) only apply to controllers that satisfied one of the following during the previous calendar year: (1) controller's annual global gross revenue exceeded $25 million; (2) controller was a data broker; or (3) controller "determined the purposes and means of processing" of personal information of at least 100,000 Massachusetts residents.
- Exempts various entities and information types, including state government entities and certain securities and futures associations; information governed by HIPAA, FCRA, FERPA, or GLBA; 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.
- Defines lawful bases for processing, including, among other things, individual consent, necessity to performance of contract with individual, and necessity to controller's compliance with legal obligation.
- Creates individual rights for consumers, including the right to access personal information; the right to obtain a portable version of personal information; the right to delete personal information; the right to correct personal information; the right to revoke consent for processing of personal information; and the right to opt out of processing for purposes of sale of personal information, targeted cross-contextual advertising, or targeted first-party advertising.
- Allows individuals to exercise their opt-out rights via browser extensions, global device settings, and opt-out preference signals.
- Prohibits controllers from processing sensitive information for purposes of sale or targeted cross-contextual or first-party advertising without individual's consent. Also generally prohibits processing of individual's sensitive information without consent, subject to limited exceptions.
- Requires data brokers to register with state AG. Data brokers that fail to register may be liable for a civil penalty of up to $500 per day, with the total penalty capped at $100,000 per year.

- Incorporates privacy by design principles, such as by requiring controllers to identify and mitigate privacy risks and harms throughout their product and service design, development, and implementation processes.
- Requires that controllers conduct risk assessments for specified processing activities, including: processing for purposes of sale of personal information or targeted cross-contextual and/or targeted first-party advertising; processing for purposes of profiling that poses certain specified risks; processing sensitive information; and any other processing "likely to result in a high risk of harm to individuals."
- Requires that large data holders include in their risk assessments analysis of the entity's use of algorithms and other artificial intelligence techniques in processing.
- Grants state AG authority to enforce the Act, including through civil actions.
- Establishes a 30-day cure period for violating entities before state AG may initiate civil action.
- State AG may seek civil penalties of up to $7,500 per violation, as well as injunctive relief. Entities that violate an injunction or order are liable for a civil penalty of up to $10,000 per violation.
- Authorizes state AG to adopt regulations to support Act's implementation.
- Creates a private right of action for individuals whose personal information is subject to a security breach "as a result of a controller's failure to implement and maintain reasonable cybersecurity controls." Individuals may seek damages (the greater of up to $500 per individual per incident or actual damages), injunctive, declaratory, and other relief.
- In security breach actions, controllers are shielded from punitive damages if they had implemented a cybersecurity program conforming to one of several enumerated frameworks, including, for example, the NIST Cybersecurity Framework.
- Establishes the Massachusetts Privacy Fund, into which civil penalties collected pursuant to the Act would be deposited.
- Subject to limited exceptions, the Act would take effect 18 months after passage. However, the Act would take effect 30 months after passage for nonprofit organizations and institutions of higher education.

Massachusetts

1. *Bill Title:* Internet Bill of Rights (HD 3245)
2. *Current Status:* As of January 29, 2023, the bill had been filed on the House docket.
3. *Key Provisions:*

- Generally, includes many provisions modeled on the GDPR.
- Applies to the "processing of personal data in the context of the activities of an establishment of a controller or a processor in [Massachusetts], regardless of whether the processing takes place in [Massachusetts]." Act also applies to the processing of personal data by controllers and processors not established in Massachusetts when the processing relates to (1) the offering of goods or services to Massachusetts data subjects; or (2) the monitoring of data subjects' Massachusetts-based behavior.

- Establishes a “right to the protection of personal data.”
- Establishes lawful bases for data processing, including, among other things, consent, performance of contract, and compliance with legal obligations.
- Incorporates privacy by design principles, such as purpose limitation and reasonable security measures.
- Prohibits the processing of specified types of sensitive personal data without consumer consent.
- Creates individual rights for consumers, including the right to access personal data; the right to correct personal data; the right to delete personal data; the right to restrict processing of personal data in specified circumstances; the right to obtain personal data in a portable format; the right to object to processing in specified circumstances (including direct marketing and profiling); and the right not to be subject to decisions based solely on automated processing that result in legal or similarly significant effects.
- Requires controllers that experience a breach involving personal data to notify the state AG within 72 hours of becoming aware of the breach. Controllers are also required to notify affected data subjects when breach is “likely to result in a high risk to the rights and freedoms of natural persons,” subject to certain exceptions (e.g., if the data was encrypted).
- Requires controllers to execute data protection impact assessments for types of processing that are “likely to result in a high risk to the rights and freedoms of natural persons” (e.g., automated processing and profiling).
- Requires that controllers and processors designate a data protection officer when: processing is executed by a public body; “core activities” of controller or processor “require regular and systematic monitoring of data subjects on a large scale; or core activities involve large-scale processing of specified types of data.
- Encourages state AG and industry groups to develop “codes of conduct” to guide entities in complying with the Act’s requirements. Allows the state AG to accredit bodies to monitor compliance with these codes.
- Requires state AG to encourage establishment of data protection certification mechanisms, seals, and marks.
- Authorizes state AG to develop standard contractual clauses for use in controller-processor and processor-subprocessor contracts.
- Imposes various requirements on transfers of personal data outside of Massachusetts. For instance, such a transfer may take place when the state AG determines that the foreign destination (including other US states) “ensures an adequate level of protection.” In the absence of such a determination, controller or processor may (subject to certain exceptions) only transfer personal data outside Massachusetts if it provides appropriate safeguards and ensures availability of data subject rights and legal remedies.
- Allows state AG to approve “binding corporate rules” to guide foreign data transfers by a particular corporate entity or group of corporate entities.
- Authorizes state AG to enforce the Act through legal proceedings.

- AG may impose administrative fines on violators. Generally, administrative fines shall be "effective, proportionate, and dissuasive." However, Act also establishes a two-tier penalty framework for specific violations: up to $10 million or 2% of worldwide annual turnover; or up to $20 million or 4% of worldwide annual turnover.
- Creates private right of action for data subjects whose rights have been infringed through a violation of the Act. Individuals have the right to receive compensation for any damage suffered as result of the violation. Data subjects may also lodge complaint with state AG.
- Authorizes state AG to promulgate rules and regulations to implement the Act.

New Hampshire

1. *Bill Title:* An Act relative to the expectation of privacy (Senate Bill 255-FN)
2. *Current Status:* As of January 29, 2023, the bill had been referred to the Judiciary Committee.
3. *Key Provisions:*

- Applies to persons that conduct business in New Hampshire or produce products or services that are targeted to residents of New Hampshire.
- Exempts various entities and information types, including state government entities; nonprofit organizations; institutions of higher education; financial institutions and data subject to GLBA; covered entities, business associates, and protected health information governed by HIPAA; controllers or processors that comply with COPPA; information governed by FCRA; information governed by the Driver's Privacy Protection Act; personal data governed by FERPA; personal data governed by the Farm Credit Act; and information governed by the Airline Deregulation Act.
- Outlines consumers' expectation of privacy including the right to confirm whether their data is being processed and access their data; the right to correct inaccuracies; the right to delete data provided; the right to obtain a copy of the personal data they previously provided to the controller in a portable and readily usable format; and the right to opt out of processing for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similar effects concerning the consumer.
- Incorporates privacy by design principles, such as purpose limitation and reasonable security practices. Controllers are further prohibited from collecting additional categories of personal information or using collected information for additional purposes without obtaining consumer consent.
- Creates additional requirements for processing sensitive data.
- Requires data protection assessments for activities that present heightened risk of harm, including the processing of data for the purposes of targeted advertisement, sale of personal information, and processing of sensitive data, among others.
- Does not create a private right of action. Violations are only enforceable by the New Hampshire AG.

- Violations of Act would constitute “unfair method of competition and unfair and deceptive acts or practices” under N.H. Rev. Stat. § 358-A:2. Violations would be subject to a civil penalty of up to $10,000 per violation, pursuant to N.H. Rev. Stat. § 358-A:4.
- Creates a sixty-day cure period after the state AG issues a notice of violation if the state AG determines that a cure is possible. If entity fails to cure violation within cure period, the attorney general may bring an action for a violation.
- Would go into effect on January 1, 2024.

New York

1. *Bill Title:* Digital Fairness Act (S2277)
2. *Current Status:* As of January 29, 2023, the bill had been referred to the Internet and Technology Committee.
3. *Key Provisions:*

- Applies to a business that engages in any activity that would subject the entity to personal jurisdiction in New York or that produces, solicits, or offers for use or sale any product or service in a manner that intentionally targets, or may reasonably be expected to contact, New York residents, and as part of such business, processes and maintains the data of 500 or more unique individuals.
- Does not provide general exemptions for entities and information governed under other federal laws.
- Creates rights for individual consumers including the right to access; right to delete; right to portability; and right to opt out of certain automated decision making; also requires the controller to obtain unambiguous opt in consent before processing and selling consumer personal information.
- Requires that controllers provide meaningful notice, which includes providing consumers, in addition to a long form privacy policy, a short form privacy policy that is accessible, clear, and concise (500 word maximum), among other requirements, upon first entering the covered business’s app or website. The short form privacy policy must include a description of the type of personal information being processed; manner in which information is processed, collected, and monetized; purpose of processing; which third-parties receive shared information; and length of data retention.
- Requires a covered business to maintain a reasonable standard of care, relative to the business’s industry, when storing, transmitting, and protecting personal information.
- Creates additional requirements for processing biometric data. Provides a limited exemption for information that is governed under HIPAA.
- Imposes additional requirements, through an amendment of the state finance law, for government usage of automated decision systems including that before adoption of such systems, government entities must engage a neutral third party to conduct an automated decision impact assessment.
- Prohibits a business from processing personal information for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially

contracting for employment, finance, health care, credit, insurance, housing, or education opportunities, in a discriminatory manner.

- Creates a private right of action. A court may award plaintiffs liquidated damages of $10,000 or actual damages, whichever is greater; punitive damages; and any other relief including injunction which the court deems appropriate.
- Violations are also enforceable by the New York AG, a district attorney, or a city attorney in a city which has population of over 750,000 people. The state AG, a district attorney, or city attorney may seek injunctive relief; restitution to redress harms to individuals or to mitigate all substantial risk of harm; and obtain civil penalties of up to $25,000 or up to 4% of the covered business's annual revenue per violation.
- Would go into effect immediately, with certain sections taking effect one year after they become law. Amendments made by this Act to the state finance law regarding discriminatory practices would take effect two years after the section becomes law.

Vermont

1. *Bill Title:* H. 121
2. *Current Status:* As of January 29, 2023, the bill had been referred to the Committee on Commerce and Economic Development.
3. *Key Provisions:*

- General Requirements for Collection and Use of Data (Sec. 2432)
    - Imposes general requirements on data collectors regarding the collection and use of personal information, including privacy-by-design principles such as data minimization and purpose limitation.
    - Provides that consumers "shall have the rights specified by rule by the Attorney General with regard to their personal information."
    - Requires data collectors that are data brokers or process data "for purposes of targeted advertising, predictive analytics, tracking, or the sale of personal information" to allow consumers to opt-out of processing for the aforementioned purposes through a universal opt-out mechanism.
- Data Broker Security Breach Notice Act (Sec. 2436)
    - Requires data brokers to notify affected consumers of data breach no later than 45 days after discovery or notification. Data brokers also required to notify state AG within 14 business days after discovery of the breach or notice to consumers, whichever is earlier.
    - Authorizes state AG and State's Attorney to investigate violations and enforce the Act.
- Document Safe Destruction Act (Sec. 2445)
    - Requires that businesses "take all reasonable steps" to destroy customer records containing PII that are no longer to be retained by the business. These requirements do not apply to entities subject to GLBA, HIPAA, or FCRA.

  - Authorizes state AG, State’s Attorney, and Department of Financial Regulation to enforce this Act, as appropriate.
- Data Broker Registration & Additional Duties (Sec. 2446, 2448)
  - Requires data brokers to register with the Secretary of State. Data brokers that fail to register are liable for a civil penalty of $100 for each day of noncompliance. Data brokers that omit required information or file materially incorrect information in their registrations are liable for additional penalties.
  - Creates rights for individual consumers to request that data brokers stop collecting data, delete data, and stop selling data. Consumers may also exercise a general opt-out covering all data brokers registered in Vermont.
  - Requires that data brokers maintain reasonable procedures to verify that brokered personal information “is used for a legitimate and legal purpose,” including identity verification and purpose certification.
  - Exempts entities and information subject to FCRA.
- Protection of Biometric Information (Sec. 2449)
  - Imposes various requirements on the collection, use, and retention of biometric identifiers, including requirements pertaining to notice, consent, and use limitation.
  - Authorizes the state AG and State’s Attorney to enforce these provisions. In addition, creates a private right of action for consumers to obtain damages and injunctive relief.
- Act would take effect on July 1, 2023.

Washington

1. *Bill Title:* People's Privacy Act (House Bill 1616)
2. *Current Status:* As of January 29, 2023, the bill had been referred to the Civil Rights & Judiciary Committee.
3. *Key Provisions:*

- Applies to businesses that conduct business in Washington, and process captured personal information and have either: a) earned or received $10,000,000 or more of annual revenue through 300 or more transactions or b) processes and/or maintains the captured personal information of 1,000 or more unique individuals during the course of a calendar year.
- Provides an exemption for certain instances and information including in the instance of a single transaction; documented emergency; to respond to a warrant or subpoena; collected, used, or stored information that is governed under HIPAA; information governed under COPPA; and employment information.
- Creates rights for individual consumers, including the right to know; the right to access and obtain the individual’s information processed by the controller; the right to refuse consent; the right to correct inaccuracies; the right to delete; and the right to not be subject to surreptitious surveillance.

- Requires unambiguous opt-in consent for the collection of personal information, as well as upon changes in the purpose or type of collection.
- Requires that controllers provide meaningful notice, which includes providing consumers, in addition to a long form privacy policy, a short form privacy policy that is accessible, clear, and concise (500 word maximum), and is available upon first engaging with the covered business's app, website, or physical space. The short form privacy policy must include a description of the type of personal information being processed; manner in which it is processed, collected, or monetized; purpose of processing; which third-parties receive shared information; and length of data retention.
- Creates additional requirements for covered businesses, as well as governmental state entities that process biometric information, such as requiring a publicly available written policy that outlines purpose and retention, among other requirements.
- Prohibits covered businesses and Washington governmental entities from processing personal information for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for employment, finance, health care, credit, insurance, housing, or education opportunities, in a discriminatory manner.
- Creates a private right of action. A court may award plaintiffs the greater of liquidated damages of $2,000 per violation or actual damages, as well as any other relief, including injunctive or declaratory relief, which the court deems appropriate.
- Violations are also enforceable by the Washington AG. The state AG may seek injunctive relief; restitution to redress harms to individuals or to mitigate all substantial risk of harm; and obtain civil penalties per violation of up to $25,000 or 4% of the covered business's annual revenue, whichever is greater.
- Enforcement provisions, including the private right of action and state AG enforcement authority, would take effect July 1, 2024. Non-profit corporations would remain exempt until July 31, 2025.

UPDATES ON EXISTING PROPOSALS

Several bills that we profiled in our previous post have since made progress in the legislative process. Key developments include the following:

- **Iowa Privacy Bill Advances through Subcommittee Vote:** A subcommittee of the Economic Growth and Technology Committee recommended passage of House Study Bill 12 by a unanimous vote of 3-0 on January 23. The bill now moves on to consideration by the full committee. House Study Bill 12 is notable in not creating a private right action, instead granting the Iowa state AG exclusive enforcement authority.
- **House Companion to Massachusetts Data Privacy Protection Act Introduced:** A House version of the Massachusetts Data Privacy Protection Act (HD 2281) was filed on the House docket on January 19. In addition, the original Senate version of the bill was re-numbered as SD 745. These bills would allow for enforcement by both the state AG and

through a private right of action. They are also notable in requiring that certain entities that use or develop covered algorithms conduct impact assessments and evaluations.

- **Tennessee Information Protection Act Referred to Committee**: The Tennessee Information Protection Act (Senate Bill 73) was referred to the Commerce and Labor Committee on January 20. The bill would be exclusively enforced by the state AG and, notably, would require that controllers and processors develop privacy programs that conform to the National Institute of Standards and Technology (NIST) privacy framework.

Contributors

Kirk J. Nahra

PARTNER

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

Ali A. Jessani

SENIOR ASSOCIATE

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

Samuel Kane

ASSOCIATE

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