
State Comprehensive Privacy Law Update – March 21, 2023

MARCH 21, 2023

The state comprehensive privacy law legislative process has officially kicked into high gear. Of course, the primary development since [our last update](#) is Iowa's passage of SF 262, which positions Iowa to become the sixth state to enact a comprehensive privacy law (joining California, Colorado, Virginia, Utah, and Connecticut). You can read our analysis of that bill [here](#).

SF 262's passage is far from the only development to report, however. Three additional bills cleared a legislative chamber in the last two weeks — the Oklahoma Computer Data Privacy Act (HB 1030), Kentucky's SB 15, and New Hampshire's SB 255. With that, there are now seven bills (besides SF 262) that have already passed a chamber this legislative session: the aforementioned Kentucky, Oklahoma, and New Hampshire bills, plus Hawaii's Consumer Data Protection Act (SB 974), Montana's Consumer Data Privacy Act (SB 384), Indiana Senate Bill 5, and New Jersey S. 332.

Finally, new bills continue to be added to the mix, with new proposals being put forth in New Jersey, New York, and Texas.

NEW PROPOSALS

Three new comprehensive privacy bills have been proposed since our last update, all in states — [New Jersey](#), [New York](#), and [Texas](#) — that already have a comprehensive privacy bill under consideration. These bills offer several unique provisions — New Jersey's NJ DATA bill, for instance, includes several provisions inspired by the GDPR (such as lawful bases for processing), while Texas's HB 4854 includes a section governing "data stream" contracts between individuals and businesses, under which individuals offer access to their personal information in exchange for benefits from the business. New York's It's Your Data Act is closer to a run-of-the-mill comprehensive privacy law, but does notably include a private right of action.

New Jersey

1. *Bill Title:* New Jersey Disclosure and Accountability Transparency Act (NJ DaTA) ([S. 3714](#))
2. *Current Status:* As of March 19, 2023, the bill has been referred to the Commerce Committee (3/13/23).
3. *Key Provisions:*

- Establishes an Office of Data Protection and Responsible Use in the Division of Consumer Affairs in the Department of Law and Public Safety. The Office would have public awareness, information sharing, and regulatory authorities.
- Exempts information subject to HIPAA, financial institutions subject to GLBA, and information governed by FCRA.
- Defines GDPR-like lawful bases for processing, including affirmative opt-in consent, performance of a contract, compliance with a legal obligation, vital interests of the consumer or another person, the public interest, and legitimate interests of a controller or third party.
- Creates GDPR-like individual rights for consumers, including: the right to access personal information; the right to correct personal information; the right to delete personal information; the right to restrict or object to processing; the right to obtain a portable copy of personal information; the right to withdraw consent to processing; and the right to lodge a complaint with the Department of Law and Public Safety.
- Prohibits the processing of sensitive information, subject to limited exceptions.
- Grants consumers an additional right not to be subject to decisions based solely on automated decision making, including profiling, that produce legal or similarly significant effects.
- Incorporates privacy by design principles, including purpose limitation and reasonable data protection safeguards.
- Requires entities to designate a “representative that shall serve as a liaison between the controller or processor and the [Office of Data Protection and Responsible Use] and public.”
- Grants the Office of Data Protection and Responsible Use the authority to adopt standard contractual clauses for use in controller-processor contracts.
- Requires entities to adopt a risk-based approach to data security.
- Requires controllers to notify the Office of Data Protection and Responsible Use within 72 hours after becoming aware of a data breach. Controllers also required to immediately notify consumers where a data breach is “likely to result in a high risk to the rights and freedoms of a person.”
- Requires controllers to conduct data protection impact assessments before processing personal information.
- Would make a violation of the Act an unlawful practice and violation of New Jersey’s consumer fraud statute.
- Grants rulemaking authority to the Division of Consumer Affairs within the Department of Law and Public Safety.
- Act would take effect on the first day of the sixth month after enactment.

New York

1. *Bill Title:* It's Your Data Act ([SB 5555](#))
2. *Current Status:* As of March 19, 2023, SB 5555 has been referred to the Senate Codes Committee (3/8/23).

3. *Key Provisions:*

- Applies to entities that do business in the state of New York; are organized for profit or financial benefit of shareholders; directly or indirectly collect personal information or contribute to determining the means of processing of collected data; and satisfy one or more of the following thresholds: (1) annual gross revenue exceeds \$50 million, (2) for commercial purposes sells or discloses the personal information of 50,000 or more consumers, households, or devices, (3) derives 50% or more of its annual revenue from selling consumers' personal information.
- Exempts various entities and information types, including nonprofit organizations, entities and information subject to HIPAA, entities subject to GLBA, and information subject to FCRA.
- Requires that covered entities provide a description of consumers' rights and designated methods for submitting requests pursuant to those rights; disclose the types of personal information a business collects, sources and methods for collection, third parties with which disclosed categories of data are shared, as well as length of retention for collected data. Entities must annually update their privacy policies.
- Creates individual rights for consumers, including the right to delete data; the right to access personal data; the right to obtain a portable copy of personal data; and the right to know the categories of personal data being shared with third parties, as well as the right to a list of such third parties.
- Incorporates privacy by design principles, including purpose limitation and reasonable security measures.
- Creates greater consumer protections against sharing of personal data. Requires entities to receive affirmative consent for the disclosure of personal information.
- Requires that entities gain affirmative consent and exercise reasonable care where information is collected for the purposes of advertisements. A violation of this provision would amount to a misdemeanor under § 50 N.Y. Civ. Rights Law.
- Creates a private right of action. Plaintiffs may recover \$750 per violation or actual damages whichever is greater, as well as injunctive or declaratory relief, and attorney fees.
- The state AG, county district attorney, or city corporation counsel may bring an enforcement action and may seek civil penalties of up to \$7,500 per intentional violation and \$2,500 for each unintentional violation.
- Would go into effect one year after the law is enacted.

Texas

1. *Bill Title:* [HB 4854](#)
2. *Current Status:* As of March 19, 2023, the bill had been filed in the House (3/10/23).
3. *Key Provisions:*
 - Applies to businesses that do business in Texas; have more than 50 employees; collect personal information of more than 5,000 individuals, households, or devices; and satisfy at least one of the following: (1) annual gross revenue exceeding \$25 million; or (2) derives

50% or more of annual revenue from processing personal information.

- Applies only to personal information collected via the Internet, a digital network, or a computing device.
- Exempts information governed by HIPAA, information governed by FCRA, information governed by GLBA, and “education information that is not publicly available personally identifiable information under [FERPA].”
- Grants the state AG rulemaking authority.
- Creates individual rights for consumers, including: the right to confirm processing of personal information; the right to access personal information; the right to obtain a portable copy of personal information; and the right to delete personal information.
- Requires businesses to delete an individual’s personal information no later than one year after the individual closes their account with that business.
- Establishes requirements for “data stream” contracts between individuals and businesses, under which individuals offer access to their personal information in exchange for benefits from the business.
- Act would generally take effect on September 1, 2023. The Act’s data deletion provisions would take effect on January 1, 2024.

UPDATES ON EXISTING PROPOSALS

Iowa’s [passage of SF 262](#) is, of course, the primary recent development with regards to existing proposals. However, as noted above, the past two weeks also saw Oklahoma’s [HB 1030](#), Kentucky’s [SB 15](#), and New Hampshire’s [SB 255](#) pass a legislative chamber (on March 8, March 15, and March 16, respectively). Notably, none of these bills create private rights of action ([an earlier version](#) of Kentucky SB 15 included a limited private right of action for individuals alleging that a controller failed to comply with a consumer rights request, but that provision appears to have been removed). Oklahoma’s HB 1030, however, would require consumers to consent to any collection of personal information by businesses — essentially establishing an opt-in consent model for all processing of personal information.

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

- **Bills That Have Cleared Legislative Chamber**
 - Hawaii’s Consumer Data Protection Act ([SB 974](#)) was referred to the House Economic Development, Consumer Protection and Commerce, and Finance Committees on March 9.
 - Montana’s Consumer Data Privacy Act ([SB 384](#)) had its first reading in the House on March 15.
 - Indiana [Senate Bill 5](#) remains under consideration by the House Judiciary Committee as of February 28.
 - New Jersey [S. 332](#) remains under consideration by the Assembly Science, Innovation and Technology Committee as of February 6.
- **Committee Referrals**
 - The three Massachusetts comprehensive privacy law proposals under consideration

this session were all renumbered and referred to various committees.

- The Massachusetts Data Privacy Protection Act ([S. 25/H. 83](#)) was referred to the Joint Committee on Advanced Information Technology, the Internet and Cybersecurity on February 16.
- The Massachusetts Information Privacy and Security Act was referred on February 16 to the Joint Committee on Economic Development and Emerging Technologies ([S. 227](#)) and the Joint Committee on Advanced Information Technology, the Internet and Cybersecurity ([H. 60](#)).
- The bill establishing an Internet Bill of Rights ([H. 1555](#)) was referred to the Joint Committee on The Judiciary on February 16.

— Committee Hearings and Calendar Placements

- The Tennessee Information Protection Act ([SB 73/HB 1181](#)) has been placed on the Senate Commerce and Labor Committee calendar for March 20 (SB 73) and the Banking and Consumer Affairs Subcommittee of the Commerce Committee's calendar for March 21 (HB 1181).
- Oregon's [SB 619](#) is scheduled for a Judiciary Committee work session on March 28.

— New Companion Bills

- [HB 1547](#), a companion bill to Florida [SB 262](#), was introduced on March 6 and referred to the Regulatory Reform and Economic Development Subcommittee of the Commerce Committee on March 9.

Authors



Kirk J. Nahra

PARTNER

Co-Chair, Artificial
Intelligence Practice

Co-Chair, Cybersecurity
and Privacy Practice

✉ kirk.nahra@wilmerhale.com

☎ +1 202 663 6128



Ali A. Jessani

COUNSEL

✉ ali.jessani@wilmerhale.com

☎ +1 202 663 6105



Genesis Ruano

ASSOCIATE

✉ genesis.ruano@wilmerhale.com

☎ +1 202 663 6154



Samuel Kane

SENIOR ASSOCIATE

✉ samuel.kane@wilmerhale.com

☎ +1 202 663 6114