
State Comprehensive Privacy Law Update – April 3, 2023

APRIL 4, 2023

The past two weeks have seen continued progress on proposed comprehensive privacy legislation across multiple states. Most notably, on March 28, Iowa Governor Kim Reynolds [signed](#) SF 262 into law, officially making Iowa [the sixth state with a comprehensive privacy law](#). Elsewhere, new bills were proposed in Louisiana, North Carolina, Pennsylvania, and Rhode Island. With Louisiana, North Carolina, and Pennsylvania's proposals, we have now seen 24 states propose comprehensive privacy legislation during this legislative session.

While no bills have cleared legislative chambers since [our last update](#), bills in Oklahoma and New Hampshire that have already passed one chamber have continued to progress in the opposite chamber. Elsewhere, bills in Tennessee, Oregon, Texas, and Florida moved forward in the committee process.

NEW PROPOSALS

Since [our last update](#), four new comprehensive privacy bills were proposed in Louisiana, North Carolina, Pennsylvania, and Rhode Island. None of the four bills contains a private right of action. The Louisiana Consumer Privacy Act, North Carolina Consumer Privacy Act, and Pennsylvania's Consumer Data Protection Act are relatively standard comprehensive privacy law proposals, but Rhode Island's Data Transparency and Privacy Protection Act includes several unique provisions. Most notably, it features a broad applicability provision, applying to any person or entity that owns a commercial website or online service that collects and maintains personal information about a Rhode Island resident.

Louisiana

1. *Bill Title:* Louisiana Consumer Privacy Act ([SB 199](#))
2. *Current Status:* As of April 2, 2023, SB 199 has been provisionally referred to the Senate Commerce, Consumer Protection, and International Affairs Committee (3/31/23).
3. *Key Provisions:*
 - Applies to controllers or processors that conduct business in Louisiana or produce a product or service targeted to Louisiana residents; have annual revenue of \$25 million or more; and satisfy one of the following: (1) control or process personal data of at least

100,000 Louisiana residents in a calendar year; (2) derive over 50% of gross revenue from sale of personal data and control or process personal data of at least 25,000 Louisiana residents.

- Exempts various entities and information types, including government entities, tribes, institutions of higher education, nonprofits, entities and information subject to HIPAA, entities and information subject to FCRA, entities and information subject to GLBA, personal data subject to FERPA, and certain employment-related information. In addition, entities are deemed compliant with the Act's parental consent requirements if they comply with COPPA's verifiable parental consent mechanisms.
- Creates rights for individual consumers, including: the right to confirm whether a controller is processing personal data and to access that data; the right to obtain a portable copy of personal data; the right to correct inaccurate personal data; the right to delete personal data; and the right to opt out of the processing of personal data for purposes of targeted advertising and sale of personal data.
- Requires that controller provide consumers with privacy notice that discloses categories of personal data processed; purposes for processing personal data; how consumers may exercise their rights; categories of personal data that controller shares with third parties; and categories of third parties with whom personal data is shared.
- Incorporates privacy by design principles, such as reasonable security measures.
- Requires that controller provide consumer with clear notice and opportunity to opt out before processing sensitive data (which includes biometric data).
- Does not create a private right of action.
- State AG has exclusive authority to enforce Act. State AG may initiate enforcement actions upon referral from the Louisiana Department of Justice's consumer protection section.
- Creates a 30-day cure period during which entities alleged to have violated Act may cure their violations before initiation of enforcement action.
- In enforcement action, state AG may recover actual damages to consumers, as well as civil fine of up to \$7,500 per violation.
- Creates a Consumer Privacy Account into which all money recovered for violations of the Act will be deposited.
- Requires that controllers conduct data protection assessments before initiating any processing that presents heightened risk of harm to consumer (including targeted advertising, selling personal data, and processing sensitive data).
- Act would become effective on December 31, 2024.

North Carolina

1. *Bill Title*: North Carolina Consumer Privacy Act ([SB 525](#))
2. *Current Status*: As of April 3, 2023, SB 525 has been filed in the Senate (4/3/23).
3. *Key Provisions*:
 - Applies to any controller or processor that conducts business in North Carolina or produces a product or service targeted to North Carolina residents; has annual revenue of

\$25 million or more; and satisfies one of the following requirements: (1) controls or processes personal data of 100,000 or more North Carolina residents in calendar year; or (2) derives over 50% of entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more North Carolina residents.

- Exempts various entities and information types, including government entities, tribes, institutions of higher education, nonprofits, entities and information subject to HIPAA, entities and information subject to FCRA, entities and information subject to GLBA, personal data governed by FERPA, and certain employment-related data. Also provides that entity in compliance with COPPA's verifiable parent consent mechanisms complies with Act's parental consent requirements.
- Creates rights for individual consumers, including the right to confirm whether controller is processing personal data and to access that data; the right to delete personal data; the right to obtain a portable copy of personal data; and the right to opt of the processing of personal data for purposes of targeted advertising or sale of personal data.
- Requires that controller provide consumers with privacy notice that includes categories of personal data processed; purposes of processing; information about how consumers may exercise data rights; categories of personal data shared with third parties; and categories of third parties with whom personal data is shared.
- Incorporates privacy by design principles, such as reasonable security measures.
- Prohibits controllers from processing sensitive personal information without providing consumer with clear notice and opportunity to opt out.
- Does not create a private right of action.
- Grants state AG exclusive authority to enforce Act. State AG may initiate enforcement action upon referral from the North Carolina Department of Justice's Consumer Protection Division.
- Creates a 45-day cure period during which entities alleged to have violated Act may cure their violations before initiation of enforcement action.
- In enforcement action, state AG may recover actual damages to consumers, as well as up to \$7,500 per violation.
- Creates a Consumer Privacy Account into which all money recovered for violations of this Act will be deposited. Act would become effective on January 1, 2024.

Pennsylvania

1. *Bill Title*: Consumer Data Protection Act ([HB 708](#))
2. *Current Status*: As of April 2, 2023, HB 708 has been referred to the House Commerce Committee (3/27/23).
3. *Key Provisions*:
 - Applies to persons that conduct business in Pennsylvania, produce goods, products or services that are sold or offered for sale to Pennsylvania residents, and control or process personal data of either: a) at least 100,000 consumers during a calendar year; or b) at least 25,000 consumers during a calendar year 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; nonprofit organizations; institutions of higher education; information governed by the Fair Credit Reporting Act; information governed by the Driver's Privacy Protection Act; personal data governed by the Family Educational Rights and Privacy Act (FERPA); personal data governed by the Farm Credit Act; and personal data collected in relation to employment. A controller that complies with the Children's Online Privacy Protection Act (COPPA) is deemed in compliance with obligations under this Act.
- Creates rights for individual consumers, including: the right to confirm whether a controller is processing personal data and to access that data; the right to delete personal data and correct inaccuracies; the right to obtain a portable copy of the consumer's personal data; 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 similarly significant effects."
- Incorporates privacy by design principles, including purpose limitation and reasonable security measures.
- Requires that controllers obtain consumer written 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; the methods by which a consumer may exercise their rights; categories of data shared with third parties and which third parties receive shared information; and a disclosure of sale and targeted advertising practices.
- Requires controllers to conduct a data protection assessment on processing activities that present a heightened risk of harm to consumers, beginning on January 1, 2024. The state AG may request any data protection assessments, but they must be kept confidential and are exempt from public inspection.
- Does not create a private right of action. Violations are only enforceable by the Pennsylvania AG's office.
- Imposes civil penalties of up to \$7,500 for each violation. The AG may recover reasonable expenses incurred in investigating and preparing the case, including attorneys' fees.
- Creates a thirty-day cure period after the AG provides written notice. If entity cures violation and provides AG express written statement, no action for statutory damages will be initiated.
- Establishes a Consumer Privacy Fund in the state treasury, into which civil penalties collected under the Act will be deposited.
- Would go into effect on January 1, 2024 or in 18 months, whichever is later.

Rhode Island

1. *Bill Title:* Rhode Island Data Transparency and Privacy Protection Act ([S 754/H 6236](#))
2. *Current Status:* As of April 2, 2023, S 754 has been referred to the Senate Commerce

Committee (3/23/23) and H 6236 has been scheduled for a hearing in the House Innovation, Internet, and Technology Committee on April 4 (3/31/23).

3. *Key Provisions:*

- Applies to any person or entity that owns a website located on the Internet or an online service that collects and maintains personally identifiable information from a customer residing in this state who uses or visits the website or online service if the website or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a website or online service on the owner's behalf or by processing information on behalf of the owner. Exempts small businesses (businesses with 10 or fewer employees).
- Exempts various entities and information types, including state government entities; nonprofit organizations; institutions of higher education; national securities associations registered under 15 USC 78o-3 of the Securities Exchange Act of 1934; financial institutions and data subject to GLBA; covered entities, business associates, and protected health information governed by HIPAA; information governed by the Fair Credit Reporting Act; information governed by the Driver's Privacy Protection Act; personal data governed by the Family Educational Rights and Privacy Act (FERPA); personal data governed by the Farm Credit Act; personal data governed by the Airline Deregulation Act, 49 USC 41713; and personal data collected in relation to employment.
- Creates rights for individual consumers, including: the right to confirm whether a controller is processing personal data and to access that data; the right to delete personal data and correct inaccuracies; the right to obtain a portable copy of the consumer's personal data; 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 similarly significant effects."
- Requires that a controller provide notice in its customer agreement or incorporated addendum or on its website or online service which includes a description of the categories of personal information being processed and the categories of data shared with third parties and which third parties receive shared information. In addition, meaningful notice includes providing consumers with a description of the categories of personal information being processed and purpose for processing, among other disclosures.
- Incorporates privacy by design principles, including purpose limitation and reasonable security measures.
- Requires data protection assessments for activities that present heightened risk of harm.
- Prohibits the processing of sensitive data without obtaining customer consent before processing sensitive data, which includes biometric data.
- Prohibits the sale of the personal data of a minor and affirms that children's data must be processed in accordance with COPPA.
- Prohibits the processing of customer personal data for targeted advertising, or the sale of personal data without customer consent.
- Does not create a private right of action. Violations are only enforceable by the Rhode Island AG's office. Disclosures of personal information in violation of this Act shall

constitute a deceptive trade practice in violation of chapter 13.1 of Title 6 Commercial Law.

- Imposes civil penalties of no less than \$100 and no more than \$500 for each intentional disclosure of personal information in violation of the Act.
- Would go into effect on January 1, 2024.

UPDATES ON EXISTING PROPOSALS

The past two weeks have seen various proposed bills continue to work their way through the state legislative process.

Of the seven bills that have already cleared a legislative chamber, the [Oklahoma Computer Data Privacy Act](#) and New Hampshire's [SB 255](#) were referred to committees, while the remaining bills' statuses remained largely unchanged.

Other bills continue to progress through the committee process. Most notable is the continued progress of the Tennessee Information Protection Act. The [Senate version](#) of this bill advanced out of committee and is scheduled for full Senate consideration on April 6, while the [House version](#) was approved by a subcommittee and is slated for committee consideration on April 4. This bill is one to track — notably, it would create an affirmative defense for businesses that implement a privacy program compliant with the National Institute of Standards and Technology (NIST) privacy framework. Elsewhere, Oregon's [SB 619](#) and the [Texas Data Privacy and Security Act](#) received committee approval on April 3 and March 20, respectively, while Florida's [HB 1547](#) received subcommittee approval on March 30.

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

– Bills That Have Cleared Legislative Chamber

- The Oklahoma Computer Data Privacy Act ([HB 1030](#)) was referred to the Senate Rules Committee on March 29.
- New Hampshire's [SB 255](#) was referred to the House Judiciary Committee on March 21.
- Kentucky [Senate Bill 15](#) had its first reading in the House on March 16.
- Montana's Consumer Data Privacy Act ([SB 384](#)) had its first reading in the House on March 15.
- Hawaii's Consumer Data Protection Act ([SB 974](#)) remains under consideration by the House Economic Development, Consumer Protection and Commerce, and Finance Committees as of March 9.
- 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 Approvals

- Both versions of the Tennessee Information Protection Act moved forward in the committee process. [SB 73](#) was passed by the Senate Commerce and Labor Committee on March 21 and has been placed on the full Senate calendar for April 6.

Meanwhile, [HB 1181](#) was passed by the Banking and Consumer Affairs Subcommittee of the Commerce Committee on March 21 and has been placed on the Commerce Committee calendar for April 4.

- Oregon's [SB 619](#) was passed by the Judiciary Committee after a work session on April 3 and referred to the Ways and Means Committee.
- The Texas Data Privacy and Security Act ([HB 4](#)) was passed by the Business and Industry Committee on March 20.
- Florida's [HB 1547](#) (a companion bill to [SB 262](#)) was reported favorably out of the Regulatory Reform and Economic Development Subcommittee of the Commerce Committee on March 30.

— **Committee Hearings and Calendar Placements**

- Florida's [SB 262](#) (a companion bill to [HB 1547](#)) has been placed on the Commerce and Tourism Committee's April 4 meeting agenda.

— **Committee Referrals**

- Texas's [HB 4854](#) was referred to the Business and Industry Committee on March 23.

— **New Companion Bills**

- A Senate version of the Minnesota Consumer Data Privacy Act ([SF 2915](#)), a companion to [HF 2309](#), was introduced on March 15 and referred to the Senate Commerce and Consumer Protection Committee.

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