Data Privacy and Security Update:
2023 and What's in Store for 2024

By Eric Rosenkoetter

This article is an excerpt from the Spring 2024 RMAI Digital Dispatch *(pages 15, 28 and 29), originally published April 2, 2024.*

Looking Back to 2023

2023 State Data Privacy Legislation

The upward trend in data privacy legislation continued in 2023. According to the National Conference of State Legislatures, "[a]t least 40 states and Puerto Rico introduced or considered more than 350 consumer privacy bills in 2023," a significant increase from the 200 bills in 2022. Many of these bills were limited in scope, relating to, for example, biometric, genetic and geolocation data, data brokers, internet service providers, etc.

"Comprehensive" consumer data privacy legislation broadly conveys certain rights to consumers and restricts the use of their personal information. Narrowing the focus to that legislation, over 60 bills were considered in almost 30 states in 2023.

Of those, seven states joined California (2018), Virginia (2021), Colorado (2021), Utah (2022), and Connecticut (2022) by enacting comprehensive data privacy legislation:

- Iowa SF 262 was enacted March 28 and goes into effect **January 1, 2025**.
- Indiana SB 5 was enacted May 1 and goes into effect **January 1, 2026**.
- Tennessee HB 1181 was enacted May 11 and goes into effect **July 1, 2024**.
- Montana SB 384 was enacted May 19 and goes into effect **October 1, 2024**.
- Texas HB 4 was enacted June 18 and goes into effect **July 1, 2024**.
- Oregon SB 619 was enacted July 18 and goes into effect **July 1, 2024**.
- Delaware HB 154 was enacted on September 11 and goes into effect **January 1, 2025**.

Although there are differences worth noting, these laws are very similar to those enacted after the California Consumer Protection Act, and most include:

- Right to access personal information
- Right to correct personal information (except Iowa)
- Right to delete personal information
- Right to obtain a portable copy of personal information being processed
- Right to opt-out of certain processing
- Data and entity-level Gramm-Leach-Bliley Act ("GLBA") exceptions (Oregon is data-level only but includes an entity-level exemption for financial institutions as defined in Or. Rev. Stat. Ann. § 706.008)
- Requirements for contracts between controllers and processors
- Risk assessments for processing certain data (except Iowa)
- No private right of action

A chart comparing the provisions of these laws can be accessed on RMAI's Privacy and Data Security Resource Center webpage.

2023 State Data Security Legislation

In 2023, six states amended their data breach notification laws.

Utah SB 127 was enacted March 23 and went into effect **May 3**. Amendments include:

- Creation the Utah Cyber Center tasked with, among other things, developing a cybersecurity plan for government agencies, identifying, assessing, and mitigating cyber threats, and promoting cybersecurity best practices;
- Requiring notification to the attorney general and the Utah Cyber Center.

Texas SB 768 was enacted May 27 and went into effect **September 1**. Amendments include:

- Shortening the time to notify the attorney general from 60 days to 30;

- Requiring notification be submitted electronically using a form provided on the attorney general's website.

Nevada SB 355 was enacted June 15 and went into effect **October 1**. The law amends Nevada's data breach notification statutes by exempting installment loan companies and making them subject to different data breach notification provisions, including:

- Determination whether notice is required is based in part on an analysis of the risk of harm to affected residents;
- The notice deadline is 30 days, as opposed to "in the most expedient time possible and without unreasonable delay";
- Breach notification by email is prohibited if a breach involves a username, password or other login credentials to an email account furnished by the licensee;
- The law specifies information that must be included in a breach notification;
- Notice must be made to the attorney general if there are more than 500 affected residents;
- There is no safe harbor for data controllers subject to and compliant with the privacy and security provisions of the Gramm-Leach-Bliley Act;
- Notice must be provided to consumer reporting agencies if the breach affects more than 1,000 persons.

Connecticut SB 1058 was enacted June 26 and went into effect **October 1**. Amendments include:

- Adding "Precise geolocation data" to the definition of "personal information";
- Depositing civil penalties into a "privacy protection guaranty and enforcement account";
- Designating a violation as an unfair trade practice under Conn. Gen. Stat. § 42-110b.

Rhode Island SB 5684 was enacted **June 27** and went into effect upon passage. Amendments include:

- Adding definitions for "classified data" and "cybersecurity incident";
- Shortening the notification period to individuals from 45 days to 15;
- Requiring notification to the state police within 24 hours;
- Specifying what must be included in a notification.

2023 State Regulation

California - In March, the California Privacy Protection Agency received approval of its first substantive rulemaking, implementing amendments to the California Consumer Privacy Rights Act. The regulations became effective **March 29**. The enforcement of some provisions were delayed by court order until March 29, 2024, but that decision was reversed by a California appellate court on February 9, 2024.

The amendments and regulations that may be of interest to RMAI members include, but are not limited to:

- A new category of personal information called "sensitive personal information" which includes Social Security and driver's license numbers;
- New content for the Notice at Collection including the categories of sensitive personal information to be collected and the purposes for which it will be used, and the length of time each category of personal information will be retained, or the criteria used to determine the retention period;
- The new right of consumers to limit the use of their sensitive personal information unless it is used for specific purposes;
- The new right of consumers to correct personal information and the requirement to include notice of that right in a privacy notice;
- Required provisions that must be included in contracts between businesses and service providers and contractors.

New York - In November, amendments to New York's Cybersecurity regulations were adopted by the Department of Financial Services with staggered implementation dates for covered entities, small businesses, and Class A companies. The amendments include:

- Creation of a category for "Class A companies" based on revenue in New York, and number of employees or global revenue;
- Heightened security measures for Class A companies;
- Annual penetration testing by a qualified internal or external party;
- Automated or manual scans of information systems;
- Risk assessments reviewed and updated annually, or more frequently as necessary;
- Multi-factor authentication for any individual accessing an information system;
- Notification to the Superintendent of any cybersecurity incident within 72 hours;
- Annual certification of compliance, or acknowledgment of noncompliance;
- Notice and explanation of extortion payments made in connection with a cybersecurity incident.

2023 Federal Regulation

GLBA Safeguards Rule - In September, the Federal Trade Commission announced its approval of an amendment to the GLBA Safeguards Rule requiring nonbank financial institutions to report to the FTC the unauthorized acquisition of unencrypted customer information involving at least 500 consumers (a "notification event"). The amendment, which becomes effective **May 13, 2024**, also provides:

- Notification must be made as soon as possible, and no later than 30 days after discovery of the event;

- Notice must be provided through an online form that will be available on the FTC's website;
- The notice must include:
  - » the name and contact information of the reporting financial institution;
  - » a description of the types of information that were involved in the notification event;
  - » if the information is possible to determine, the date or date range of the notification event;
  - » the number of consumers affected or potentially affected by the notification event;
  - » a general description of the notification event; and
  - » whether any law enforcement official provided a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the Federal Trade Commission to contact the law enforcement official.

What's in Store for 2024

Comprehensive Consumer Data Privacy Legislation

On January 16, 2024, New Jersey S 332 was enacted and goes into effect **January 1, 2025**. Additionally, as of this writing, New Hampshire SB 255 is eligible for the Governor's signature and, if enacted, will also go into effect **January 1, 2025**. Both are similar to the 2023 laws described above and include entity and data level GLBA exceptions with no private right of action.

The RMAI Data Privacy & Security Working Group ("Working Group") is currently tracking over 60 comprehensive data privacy bills and draft regulations in California concerning risk assessments and automated decision making technology.

Data Security

The Working Group is tracking almost 20 bills that would amend state data breach notification laws. Common proposed amendments include requiring notification to the attorney general in the event of a breach and shortening the timeframe for notification.

Artificial Intelligence

The hot topic in 2024 is Artificial Intelligence ("AI") with its opportunities for greater innovation and efficiencies. With that, though, comes the potential for abuse and unintended consequences. The federal government, law enforcement officials, along with state legislators and regulators have shown a keen interest in both sides. To date, almost 300 bills have been introduced in the states to study or regulate the development and deployment of AI. Many focus on the use of AI by government agencies or regulation with respect to deepfakes, election campaigns, and employment decisions.

The Working Group is focusing its attention on legislation that may more directly affect RMAI members, such as that which:

- allows consumers to opt out of communications utilizing AI chatbots;
- provides consumers the right to know if and how AI is being used for certain decision-making and the right to opt out;
- requires risk assessments if AI is used for decisions related to creditworthiness or the availability of financial products or services;
- prohibits using automated decision tools that result in algorithmic discrimination.

Conclusion

2024 promises to be an eventful year with respect to data privacy, security legislation and regulation of the use of artificial intelligence. Effective dates to keep in mind this year include the following:

May 13:

- GLBA Safeguards Rule Data Breach Notification Amendments

July 1:

- Oregon Data Privacy Act
- Tennessee Information Protection Act
- Texas Data Privacy and Security Act

October 1:

- Montana Consumer Data Privacy Act

Eric Rosenkoetter
Principal
Maurice Wutscher LLP

Eric Rosenkoetter is a principal at Maurice Wutscher LLP, where he provides counsel to businesses nationwide. For many years, he has focused his practice on compliance and advocacy related to consumer financial services. Eric enjoys the privilege of managing RMAI's bright and energetic Data Privacy and Security Working Group.