FORC
FEDERATION
OF
REGULATORY
COUNSEL

The State of Data Privacy in the U.S.

Fred E. Karlinsky, Esq.
Greenberg Traurig, P.A.
(954) 768-8278 | karlinskyf@gtlaw.com

Timothy F. Stanfield, Esq.
Greenberg Traurig, P.A.
(850) 425-8547| stanfieldt@gtlaw.com

Christian Brito, Esq.
Greenberg Traurig, P.A.
(954) 768-8279 | britoc@gtlaw.com

The risks associated with data collection and processing are at an all-time high. Data protection is a high-stakes game that is difficult to track since there is no universal legal requirement to disclose information related to data breaches. Newly released research from IBM shows that the average global cost of a single data breach in 2023 is $4.45 million.[1]

Across the globe, policymakers are holding organizations accountable for protecting private data. Data privacy laws are designed to regulate the collection and use of consumer data and establish consumer protections as it relates to their personal information. The European Union was the first major governmental body to enact comprehensive data privacy protections with the adoption of the General Data Protection Regulation (GDPR) in 2018. The GDPR sets guidelines for the collection and processing of personal information of individuals who live in the European Union.

The United States has so far taken a different path. In the United States, federal data privacy protections are not comprehensive but, instead, are focused on specific policy areas. The rules that govern privacy protections related to health information are an example of the United States' policy area-specific approach to data privacy. The Health Insurance Portability and Accountability Act (HIPAA) protects patients' "protected health information" by imposing privacy and security standards on "covered entities", including hospitals, physicians and other healthcare providers. Similarly, the Family Educational Rights and Privacy Act (FERPA) enacted in 1974, provides protections for student immunizations and other school health records. HIPPA and FERPA are two good examples of the United States federal government's policy of addressing data by policy areas instead of adopting a comprehensive data privacy framework like has been done with the GDPR in the European Union.

The lack of comprehensive action on data privacy by the United States federal government has forced states to address the issue and adopt comprehensive data privacy standards on a state-by-state basis. Generally, comprehensive state data privacy laws afford consumers rights that govern how their data is processed and stored while imposing standards on businesses that process and control consumer data.

Currently, four states (California, Colorado, Connecticut and Virginia) have comprehensive data privacy laws in effect, while seven more comprehensive state data privacy laws (Indiana, Iowa, Montana, Oregon, Tennessee, Texas and Utah) will become effective between the end of 2023 and January 1, 2026.

California led the states with the adoption of the California Consumer Privacy Act (CCPA) in 2018 and with voter approval of the California Privacy Rights Act (CPRA) in 2020. The CCPA provided consumers more control over the personal information businesses collect about them and established rights for California consumers, including:

1. the right to know about the personal information a business collects about them and how it is used and shared;
2. the right to delete personal information collected from them (with some exceptions);
3. the right to opt out of the sale of their personal information; and,
4. the right to non-discrimination for exercising their CCPA rights.

The CPRA amended the CCPA by expanding the criteria for application of the law and by imposing additional requirements on businesses that collect consumer data, including requirements related to data retention, data minimization and requirements to relay consumers' deletion requests to service providers and third parties to whom consumer data has been sold.

Most states have used the CCPA and CPRA as models for comprehensive data privacy legislation since they were adopted by California. Most of the consumer rights and commercial obligations imposed by states are substantially similar to those imposed by the CCPA and CPRA. The most notable distinction between the states is "who" the laws apply to. After the adoption of the CPRA, California's data privacy laws apply to any company in California that exceeds $25 million in gross revenue in the preceding calendar year; any company that buys, sells, or shares the personal information of 100,000 or more consumers or households in California; or any company that derives 50% or more of its annual revenue from selling or sharing consumers' personal information. The other three states that enforce state data privacy laws all apply to businesses that control or process the personal data of a minimum number of residents of each state. However, while California, Virginia and Connecticut also have criteria related to the amount of revenue generated by the sale of personal information for determining whether the law applies to a commercial entity, Colorado's statute does not consider how much revenue a business generates from the sale of personal data. This lack of consistency in determining the application of state data privacy laws means businesses must be mindful to review the data privacy laws in any state they operate in to decide whether or not they are subject to that state's data privacy laws.

This jagged patchwork of federal and state laws and regulations related to data privacy can be problematic for companies doing business in the United States, forcing companies to comply with varied and, sometimes, competing requirements.

In an effort to foster the implementation of a uniform set of standards to regulate the manner in which companies use and store consumer data, the National association of Insurance Commissioners (NAIC) has developed three model laws: the Insurance Information and Privacy Protection Act #670, the model Privacy of Consumer Financial and Health Information Regulation #672 and the Standards for Safeguarding Customer Information Regulation #673. The NAIC also adopted the Insurance Data Security Model Law #668 which complements the aforementioned NAIC data privacy models. We will explore each of these models, in turn.

The NAIC's Insurance Data Security Model Law #668 establishes data security standards for regulators and insurers to mitigate the potential damage of a data breach. The model law applies to insurers, insurance agents and other entities licensed by a state department of insurance. The Model requires insurers and other entities licensed by a department of insurance to develop, implement and maintain an information security program, investigate cybersecurity events, and notify the state insurance commissioner of such occurrences. Model Law #668 has been adopted by Alabama, Connecticut, Delaware, Indiana, Iowa, Louisiana, Maine,

Maryland, Michigan, Minnesota, Mississippi, New Hampshire, New York, North Dakota, South Carolina, Tennessee, Kentucky, Vermont, Virginia,
Wisconsin and Ohio.

The Insurance Information and Privacy Protection Model Act #670 establishes guidelines for notifying consumers about information practices; authorizing the disclosure of a consumer's information; disclosing a consumer's personal information; accessing consumer personal information held by insurers or insurance producers; correcting, amending, and deleting consumer information, and explaining and documenting adverse underwriting decisions. Arizona, California, Connecticut, Georgia, Illinois, Maine, Massachusetts, Nevada, New Jersey, North Carolina, Ohio, Oregon, Virginia, Kansas, Minnesota and Montana have adopted all or portions of Model Law #670.

The Privacy of Consumer Financial and Health Information Regulation #672 provides guidelines and processes for collecting and processing consumer health and financial information used in underwriting and claims determinations. The Model requires insurers to provide consumers with initial privacy notices, annual privacy notices, opt-out notices and authorizations for the disclosure of information. Model law #672 was adopted by all states so that they can comply with the Gramm-Leach-Bliley Act.

Finally, the NAIC's model Standards for Safeguarding Customer Information Regulation #673 creates standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality, and integrity of customer information, pursuant to the Gramm-Leach-Bliley Act. Under the Model, licensees must implement an information security program, assess their own internal and external risk factors and implement a program to manage their risk, including risks created by third parties. To date, 34 states have adopted Model Law #673 or a substantially similar law.

Despite the efforts of the NAIC to address consumer data privacy issues, advances in technology and the manner in which companies collect and utilize data have quickly outpaced any advances made by the NAIC in implementing its data privacy models. To address contemporary trends in the application of consumer data, the NAIC's Privacy Protections (H) Working Group is drafting Insurance Consumer Privacy Protection Model Law #674. The working group is taking a collaborative approach to the drafting process and collecting feedback from various stakeholders, including consumer and industry representatives, state attorney generals and Congress. The goal of Model #674 is to replace the older model laws with a modernized model law incorporating current standards and concepts that are prevalent incurrent data privacy laws.

On February 1, 2023, the Working Group released an exposure draft of Model #674. The Model establishes standards for insurance licensees and third-party administrators for the collection, processing, retaining, or sharing of consumers' personal information. The Model restricts the collection, processing, retention and sharing of personal information for purposes related to insurance transactions and imposes a requirement that unnecessary data be deleted within 90 days. Licensees and third-party administrators will be required to establish oversight of service providers and impose contractual standards for data collection and management. Model #674 expands consumer data rights by establishing that a consumer has a right to have their personal information amended, corrected, or deleted under most circumstances. The definition of "personal information" is substantially expanded to include "sensitive personal information", "health information" and "biometric information." The term "sensitive personal information" is defined as "information that reveals (i) a consumer's social security, driver's license, state identification card, or passport number; (ii) a consumer's account log-in or financial account, debit card, or credit card numbers in combination with any required security or access code, password, or credentials allowing access to an account; (iii) a consumer's precise geolocations; (iv) a consumer's racial or ethnic origin, religious, or philosophical beliefs; (v) union membership; (vi) the contents of a consumer's personal mail, personal email and personal text messages unless the person in possession is the intended recipient of the communication;

(vii) a consumer's genetic data; (viii) a consumer’s sex life or sexual orientation; (ix) a consumer’s citizenship or immigration status; (x) a consumer’s health information; or (xi) a consumer's biometric information. Insurance licensees and third-party administrators are prohibited from selling "personal information" and engaging in marketing with "sensitive personal information" under the Model.

The NAIC's Privacy Protections (H) Working Group accepted comments on Model Law #674 through August of 2023. The Working Group is expected to release a revised version of the Model before the end of the year.

Given the pace of technological innovation and the ever-evolving commercial use of personal data, it is safe to say that data privacy regulation in the United States is still in its infancy. Navigating the patchwork of state and federal data privacy regulations is daunting for the most sophisticated of businesses. As regulators, legislatures and Congress consider new laws and regulations, they must carefully balance innovation by insurers and insurance servicers with the rights of consumers to control their data. As the debate rages on whether Congress should adopt a single comprehensive data privacy law to replace current laws, insurers and others working in and around the insurance industry must strive for compliance with the existing state and federal patchwork of data privacy laws.

REFERENCES

[1] IBM Security, The 2023 Cost of a Data Breach Report (July 24, 2023), https://www.ibm.com/security/data-breach