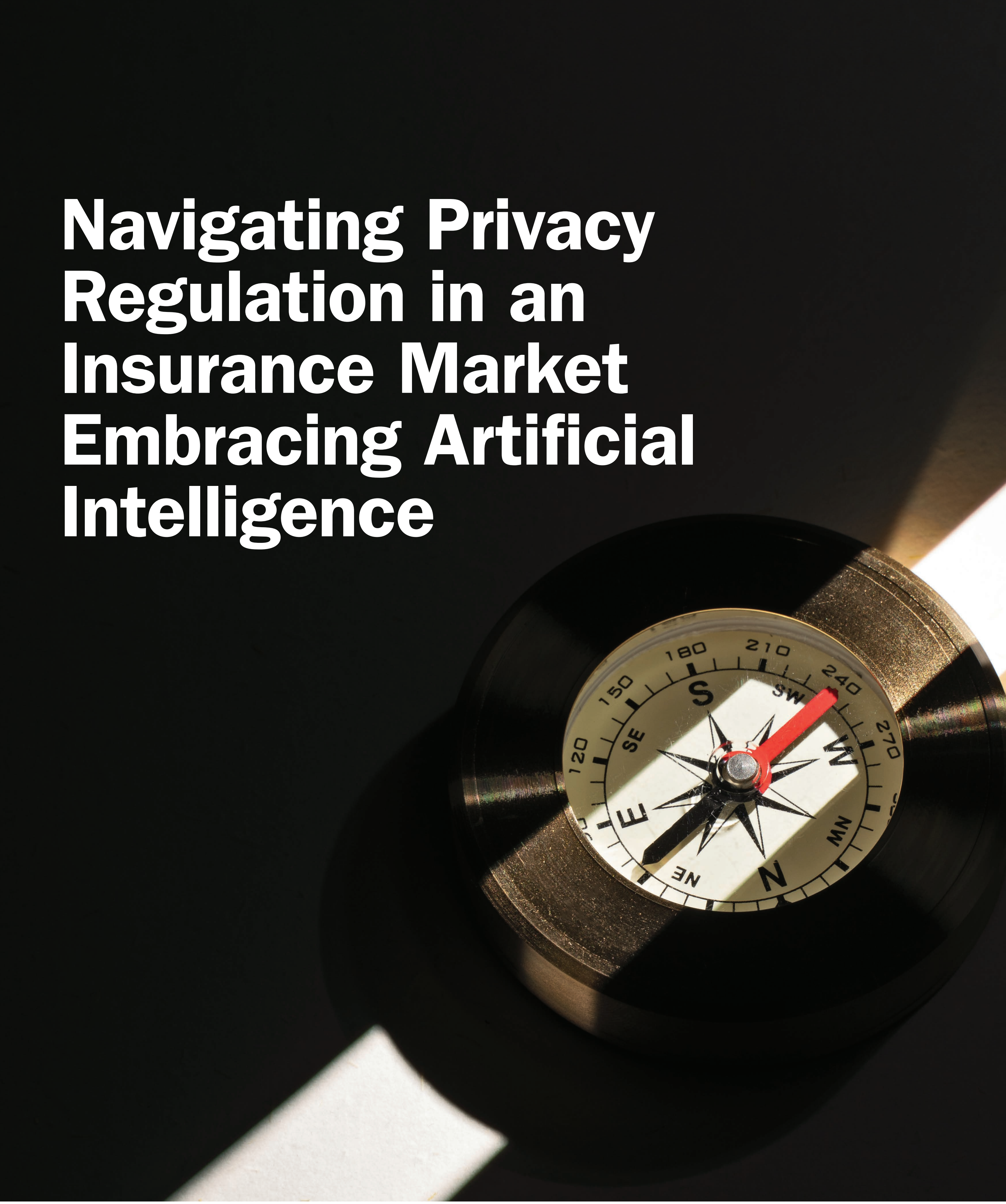
Navigating Privacy Regulation in an Insurance Market Embracing Artificial Intelligence



By Fred E. Karlinsky, Timothy F. Stanfield, Christian Brito, and Jordan J. Luczaj

MIRAGEC/MOMENT VIA GETTY IMAGES

Technology evolves every day, continuously advancing and changing industries in the United States and across the globe. Anyone who doubts this need only look to the artificial intelligence (AI) revolution that is currently unfolding. With all the benefits and powers of these tools come significant drawbacks and concerns to be navigated. This is especially true for the insurance sector. One of regulators' primary concerns with the adaptation of big data and technology has been protecting consumers' data from exposure. As such, it is important to examine the current landscape of data privacy regulations and understand why they continue to be of critical importance.

As is frequently the case, the technology in the commercial sector has seemingly advanced beyond current regulation. Initially, this was observed in the realms of data and cybersecurity, and now regulatory bodies are increasingly shifting their focus to AI. However, the reality is that the utilization and regulation of data, cybersecurity, and AI are interconnected. Thus, a comprehensive understanding of one topic requires consideration of the other.

Although interested parties recognize the importance of data privacy compliance in risk management, balancing the goals of customer protection and market stabilization while avoiding requirements that will stifle innovation and progress can be challenging. Until the emergence of comprehensive data privacy regulations, IT departments were primarily responsible for compliance with handling data-related tasks. However, the shifting emphasis to concentrations of large swaths of data has compelled top legal professionals to assume the responsibility of managing this significant area of risk.[1] Consequences for noncompliance can vary from steep fines to potential reputational damage and even the loss of faith and trust.

With the lack of an overarching data privacy framework in the United States, organizations must be aware of recent developments at the state level, as well as international privacy laws, which could apply and may serve as examples for future U.S. legislation. This article examines the developments in Europe and the United States, including both federal and state privacy laws and regulations, and discusses potential future developments in data privacy regulatory regimes.

Modern Risks in the Insurance Sector

To evaluate the regulatory landscape and ascertain how effectively existing privacy regulations address modern risks, it is essential first to examine the risks associated with modern technology, such as AI adoption, in the insurance sector and consider whether they differ from those linked to traditional insurance.

Concerns regarding transparency and explainability are long-standing in the insurance industry.[2] In many jurisdictions, existing insurance and related regulations require clear communication of financial products to consumers.[3] However, recent technological advancements, coupled with

TIP: Insurers should continuously monitor evolving privacy laws and update data governance practices to avoid compliance gaps and regulatory exposure.

input from novel data sources and types, have underscored the significance of these issues even further.[4]

Insurers collect and store vast amounts of sensitive customer data, which is crucial for conducting their business, making them a prime target for cybercriminals. Further, insurers may incidentally harness the data used for predictive analytics to encroach upon private information to which they legally should not have access.[5] Utilizing AI platforms in their practice creates yet another access point of which this data could be targeted. Integrating the data on these platforms likely necessitates compliance with data privacy laws. This is just one example of how modern technology and business practices require proactivity by the insurers in establishing comprehensive data protection measures to secure customer information, prevent unauthorized access, and implement protocols for addressing potential breaches.

European Developments in Privacy Law

The preeminent example of a comprehensive data privacy law is the European Union's (EU's) General Data Protection Regulation (GDPR).[6] This regulation became effective on May 25, 2018, and is arguably the toughest data privacy law in the world. However, as the name suggests, the GDPR also has elements of data security baked into its core. And even though it was drafted and passed by the EU, the GDPR imposes obligations that apply to extraterritorial organizations anywhere in the world, so long as they target or collect data related to people in the EU.[7] Hence, a significant percentage of U.S. businesses are subject to the GDPR.

Fred E. Karlinsky *is a shareholder and chair of Greenberg Traurig's global insurance regulatory and transactions practice group. He has over 30 years of experience representing the interests of insurers, reinsurers, and a wide variety of other insurance-related entities. He may be reached at karlinskyf@gtlaw.com.* **Timothy F. Stanfield** *is a shareholder with Greenberg Traurig's Florida government law and policy practice. His practice is largely focused on regulated industries, including insurance, land use, and alcoholic beverages. He may be reached at stanfieldt@gtlaw.com.* **Christian Brito** *is of counsel with Greenberg Traurig, where he focuses his practice on national insurance regulatory and compliance matters. He may be reached at christian.brito@gtlaw.com.* **Jordan J. Luczaj** *is an associate at Greenberg Traurig, where he focuses his practice on regulatory matters involving federal and state securities and insurance laws. He may be reached at jordan.luczaj@gtlaw.com.*

The GDPR imposes significant obligations on entities that collect, use, store, share, or process personal data of individuals in the EU or the European Economic Area (EEA).[8] There are significant recordkeeping requirements as well as limitations on data retention.

The GDPR is lengthy, complex, and surprisingly light on specifics, making GDPR compliance a daunting prospect, particularly for small and medium-sized enterprises. Pursuant to the GDPR, if a company processes personal data of individuals in the EU or EEA, it must do so according to a lengthy list of protection and accountability principles, which may be best summarized by saying that a company's data collection, data usage, and recordkeeping processes must be fair, transparent, accurate, and narrowly tailored to meet a legitimate purpose that has been disclosed to the data subject.[9] For most businesses, evaluating practices and conducting activities that are required to achieve compliance can take several months or years.[10] The GDPR includes the potential for harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.[11]

The GDPR does not refer to citizens or EU citizens. Indeed, the language that is used most consistently throughout the GDPR is "natural person" or "data subject." A data subject is an "identified or identifiable natural person" from or about whom information is collected.[12] This is because the GDPR stipulations apply when personal data is processed of a data subject who is in an EU country at the time the data is processed. Article 3(1) states: "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."[13] Therefore, a controller or processor based in the EU that processes data of data subjects located anywhere in the world can also expect the GDPR to apply. There are some enumerated exceptions to the GDPR's broad coverage, such as the household activity exception, member state–enacted exceptions for freedom of expression and journalism, and areas such as national security and policing.[14] But, the default scope of the GDPR's coverage remains extremely broad.

The EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. Data Privacy Framework (UK Extension to the EU-U.S. DPF), and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) were developed to facilitate transatlantic commerce by providing U.S. organizations with reliable mechanisms for personal data transfers to the United States from the EU or EEA, the United Kingdom (and Gibraltar), and Switzerland that are consistent with the respective laws.[15] The Data Privacy Framework (DPF) Program, which is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce, enables eligible U.S.-based organizations to self-certify their compliance pursuant to the EU-U.S. DPF and, as applicable, the UK Extension to the EU-U.S. DPF and/or the Swiss-U.S. DPF.[16] To participate in the DPF Program, a U.S.-based organization is required to self-certify to the ITA via the DPF Program website and publicly commit to comply with the DPF Principles.[17] While the decision by an eligible U.S.-based organization to self-certify its compliance and participate in the relevant parts of the DPF Program is voluntary, effective compliance upon self-certification is compulsory.[18] Once such an organization self-certifies to the ITA and publicly declares its commitment to adhere to the DPF Principles, that commitment is enforceable under U.S. law.[19]

For insurers, the focal point should be on the new obligations for data controllers. The responsibility for ensuring that rules are complied with is now shared between data controllers and data processors.[20] Previously, the onus was on data controllers regarding the processing of the personal data they controlled.[21] And while the burden is still on the controller to enter into contracts, both data controllers and data processors can be on the hook for failing to comply with the GDPR. Given that most insurance providers are data controllers that rely on third-party processing, it is therefore imperative that any contracts between insurance companies and their data processors be regularly updated to reflect the responsibilities and liabilities of each entity regarding data processing and GDPR compliance.

Federal Developments in Privacy Laws in the United States

Existing domestic privacy rules governing subsets of the population or specific categories of data can serve as useful guides for the needed updates to general consumer data privacy regulations. The rules that govern the use and management of personal health information are a great example of the federal government's industry-specific approach to data privacy regulation. The Health Insurance Portability and Accountability Act (HIPAA) is the United States' primary health privacy and security law. Passed in 1996, HIPAA includes both data privacy and security standards.[22] In addition to HIPAA, separate privacy laws govern specific areas of the U.S. health care system. For example, student immunizations and other school health records are generally covered by the Family Educational Rights and Privacy Act (FERPA), which was enacted in 1974.[23] FERPA intersects with and sometimes conflicts with the Children's Online Privacy Protection Act (COPPA), which protects data of children under the age of 13.[24] These laws, while effective within their respective areas of focus, fall short of implementing comprehensive requirements on a national level.

American Privacy Rights Act. On April 5, 2024, two key members of U.S. Congress released a draft bipartisan, bicameral federal privacy bill called the American Privacy Rights Act (APRA).[25] A little more than two years removed from the last significant attempt to forge a national privacy law, Representative Cathy McMorris Rodgers (R-WA), chair of the House Committee on Energy and Commerce, and Senator Maria Cantwell (D-WA), chair of the Senate Committee on Commerce, Science, and Transportation, went on the record to discuss the newly released draft legislation.[26] They also published a press release, in which they stated:

> This bipartisan, bicameral draft legislation is the best opportunity we've had in decades to establish a national data privacy and security standard that gives people the right to control their personal information . . . . It strikes a meaningful balance on issues that are critical to moving comprehensive data privacy legislation through Congress.[27]

The bill purports to establish foundational uniform national data privacy rights for Americans by putting people in control of their own personal data, eliminating the patchwork of state laws by setting one national privacy standard, minimizing the data that companies can collect and use about people to what companies actually need to provide them services, and finally, giving Americans control over where their personal information goes by including the ability to prevent the transfer or selling of their data.[28] The bill also allows individuals to opt out of data processing if a company changes its privacy policy.[29] This provides stricter protections for sensitive data by requiring affirmative express consent before sensitive data can be transferred to a third party, and requires that companies allow people the ability to access, correct, delete, and export their data. Such a measure would also allow individuals to opt out of targeted advertising.

The initial draft of the bill would accomplish greater protection of civil rights by bestowing enforceable data privacy rights.[30] It gives individuals the right to sue persons who violate their privacy rights and recover money for damages when they've been harmed.[31] It also has a provision preventing companies from enforcing mandatory arbitration in cases of substantial privacy harm.[32] "Substantial privacy harm" includes using people's personal information to discriminate against them on the basis of race, color, religion, national origin, sex, or disability.[33] For example, a company might use individuals' personal private information for targeting or exempting them from ads and algorithms. Further, it would allow individuals to opt out of a company's use of algorithms to make decisions about housing, employment, health care, credit opportunities, education, insurance, or access to places of public accommodation. Finally, annual reviews of the companies' algorithms would help ensure that the algorithms do not put individuals at risk of harm and remediate discrimination.

The bill would also hold companies accountable by establishing strong data security obligations. These measures include strong data security standards that aim to prevent data from being hacked or stolen. It also ensures that individuals know when their data has been transferred to foreign adversaries, and authorizes the Federal Trade Commission, individual states, and consumers to enforce against violations.[34] Notably, small businesses that are not selling their customers' personal information are exempt from the requirements of this bill.[35]

However, just before a committee markup session in the summer of 2024, the bill underwent several contentious revisions. As a result, the following revisions were made:

- The section addressing civil rights protections was removed.[36]
- The sections related to AI and algorithms were removed.[37]
- Sections regarding "privacy by design" requirements and responsibilities for data brokers and enabling users to request that humans rather than algorithms make "consequential decisions" were added.[38]

The removal of civil rights protections provisions in particular led dozens of data privacy, internet rights, and civil rights groups to express objections or withdraw support.[39] And even after the changes, Republican leadership signaled they would not support the bill, leading the markup session to be canceled.[40] With political gridlock as a formidable obstacle, it seems much more likely that state-level initiatives will pass rather than a comprehensive federal framework.

Existing domestic privacy rules governing subsets of the population or specific categories of data can serve as useful guides for the needed updates to general consumer data privacy regulations.

U.S. federal cybersecurity. On March 2, 2023, President Biden released the National Cybersecurity Strategy, a guiding document that set the course for how the Biden-Harris administration drove policy.[41] The Office of the National Cyber Director (ONCD) worked to coordinate implementation of the 69 initiatives identified in the first iteration of the strategy's implementation plan.[42] Federal agencies made progress on all 69 initiatives, completing more than 20 within the first year.[43] A second version of the National Cybersecurity Strategy, released on May 7, 2024, added 31 new initiatives.[44] By then, 92% of the initiatives that were scheduled to be completed by that point in time had been completed.[45] In June 2025, the Trump administration issued a cybersecurity executive order that amends, rather than displaces, the Biden administration's initiatives.[46] While the new order preserves core themes of securing federal systems, it pares back some prescriptive mandates for agencies, and overall shifts toward a more discretionary posture.[47]

The rapid pace of technological advancements poses challenges for regulators to ensure that fair and ethical practices are used.[48] In the pursuit of establishing the configuration for a control environment, governmental bodies and regulatory authorities encounter the challenge of disparate and frequently inharmonious approaches.[49] Consequently, insurance organizations face obstacles to effectively navigate through these discrepancies, thereby fostering significant levels of uncertainty.

The Securities and Exchange Commission (SEC), on July 26, 2023, adopted rules requiring registrants to disclose material cybersecurity incidents they experience and material information regarding their cybersecurity risk management, strategy, and governance on an annual basis.[50] The SEC also adopted rules requiring foreign private issuers to make comparable disclosures. The rules require registrants to disclose on the new Item 1.05 of Form 8-K any cybersecurity incident they determine to be material and to describe the material aspects of the incident's nature, scope, and timing, as well as its material impact or reasonably likely material impact on the registrant.[51] An Item 1.05 Form 8-K will generally be due four business days after a registrant determines that a cybersecurity incident is material.[52]

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was signed into law by President Biden in March 2022 as part of the Consolidated Appropriations Act of 2022.[53] CIRCIA includes a number of requirements related to the required reporting and sharing of covered cyber incidents. First, there is a reporting requirement that the Cybersecurity and Infrastructure Security Agency (CISA) must develop and issue regulations requiring covered entities to report back to CISA on any covered cyber incidents within 72 hours from the time the entity reasonably believes the incident occurred.[54] Additionally, any federal entity receiving a report on a cyber incident after the effective date of the final rule must share that report with CISA within 24 hours.[55] CISA will also have to make information received under CIRCIA available to certain federal agencies within 24 hours.[56] The Department of Homeland Security was also prompted to establish and chair an intergovernmental Cyber Incident Reporting Council to coordinate, deconflict, and harmonize federal incident reporting requirements.[57]

The enactment of CIRCIA marked an important milestone in improving America's cybersecurity by requiring CISA to develop and implement regulations requiring covered entities to report covered cyber incidents and ransom payments. These reports have allowed CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims.

State Developments in Privacy Laws in the United States

To date, the United States does not have a central, widely applicable federal general consumer data privacy law or a data security law. Instead, there are several subject matter, sector, or industry-specific federal privacy laws, as well as a new generation of consumer-oriented privacy laws coming from the states.

NAIC model privacy laws. One of the main purposes of the National Association of Insurance Commissioners (NAIC) is to help achieve some level of uniformity among state laws and regulations governing the U.S. insurance industry, which is primarily regulated at the state level. The NAIC promotes uniformity through the development and implementation of model laws and guidance to be adopted by the states. It should come as no surprise, then, given the flurry of data privacy activity at the state level, that the NAIC is working on a data privacy model law.

On February 1, 2023, the NAIC's Privacy Protection Working Group released a first draft of the Insurance Consumer Privacy Protection Model Law #674 during the NAIC 2023 Spring National Meeting.[58] It was drafted with the objective to supersede NAIC Insurance Information and Privacy Protection Model Act #670 and the Privacy of Consumer Financial and Health Information Regulation #672, which have been in place for decades and have been widely adopted by member states. The objectives of Model Law #674 include: (1) enhancing transparency regarding how a consumer's data is collected, processed, shared, and retained; (2) requiring consumer consent before personal information is shared with other entities, especially those outside the United States with potentially nonconforming privacy protections (potentially impacting current affiliate sharing practices in the industry); (3) prohibiting insurers from selling consumers' personal information; (4) ensuring that consumers have the right to amend or correct their personal information unless the insurer can show good cause for refusal; (5) adding a record retention requirement instead of a "right to be forgotten" provision, which is common in recent state consumer data protection laws; and (6) emphasizing the oversight responsibility of third-party service providers, making it clear that this oversight remains primarily with the licensed insurer.[59]

Model Law #674 is extraordinarily broad in scope and, where adopted by states, is fundamental to how insurance-regulated entities conduct business. Notably, it includes a safe harbor provision for entities complying with HIPAA and an optional private right of action. Many concepts in Model Law #674 are derived from recent state privacy laws.

When the working group exposed Model Law #674 for a public comment period, it received significant pushback, with many parties submitting written comments. Originally, upon reviewing the comments, the working group set out to revise Model Law #674, but it seems those efforts have stalled. In June 2024, the working group took a vote and decided to stop work on Model Law #674 and instead put their efforts into reviewing and revising Model Law #672.[60]

NAIC model data security law. In October 2017, the NAIC approved an Insurance Data Security Model Law (IDS Model Law).[61] The NAIC's model law establishes a legal framework for requiring insurance organizations to operate complete cybersecurity programs, including everything from planned cybersecurity testing and board-level involvement in the information security program to incident response plans and specific breach notification procedures.[62]

First and perhaps most important, the NAIC model law requires a company's board of directors to oversee its information security program. Even if executive management delegates responsibilities to an individual or committee, the board is still required to "receive a report from the delegate(s) complying with the requirements" and to annually report on the overall status of the security program.[63] Although the New York Department of Financial Services (NYDFS) has similar regulations, the NAIC language is stronger and more direct about the role of the board.

The IDS Model Law, however, only states that organizations must, "no less than annually, assess the effectiveness of the safeguards' key controls, systems and procedures."[64] Once the law is adopted and implemented, these requirements might be more specific; but for now, the NAIC is vague about what kind of annual assessments are required. Perhaps the most detailed requirements in the IDS Model Law are those related to notifying the state's insurance commissioner in the case of a cybersecurity event. Almost any event that involves the nonpublic information of 250 or more customers must be reported to the insurance commissioner within 72 hours of discovery.[65] Additionally, the NAIC provides a list of 13 categories of information that must be reported in the case of an event, including the date it occurred, how it was discovered, what data was accessed or lost, and the estimated number of customers affected.[66]

Currently, half of the states have adopted some form of the model law in a substantially similar manner.[67] This requires states to adopt the model in its entirety but does allow for variations in style and format. Additionally, some states, including Maryland, New York, and Puerto Rico, have undergone activity that is related to the model law, such as other administrative guidance like bulletins and notices.[68]

What to Expect in Future Privacy Regulation

With the lack of an overarching federal legal or regulatory framework, privacy laws will continue to be created and expanded upon at the state level. While this approach may allow states to innovate and develop laws that suit their own needs and objectives, a state-by-state approach has created a patchwork of overlapping and often conflicting regulatory standards, as opposed to fostering a collaborative mechanism for states to work together to find uniform solutions. This is unlikely to change in the wake of the ongoing implementation of the priorities of the new presidential administration, as the federal government's failure to pass comprehensive privacy laws is not a problem that can be attributed to any single political party or administration. Thus, in 2025, compliance, legal, and regulatory teams must continue to monitor state legislative activity on privacy and develop protocols to ensure that their organizations are complying with the ever-expanding list of applicable laws and regulations. That is especially true for companies that operate across multiple states or internationally.

With rapidly evolving technology, the need to stay abreast of ever-changing state standards is even more pronounced. Current regulations and guidelines for modern technology and data privacy in the insurance industry primarily revolve around data protection, transparency, fairness, and accountability. Insurers must stay proactive and respond to evolving technology and its impact on the industry. Understanding the intricacies of new technology, addressing biases, safeguarding data privacy and security, and fostering collaboration are key considerations for the insurance sector and regulators. A collaborative approach will enable regulators to keep up with emerging trends and assist in the design of effective regulations. By striking the right balance between innovation and regulation, insurers and regulators can harness the potential of modern technology to improve the products and experience for the consumer. ◀

Notes

1. James Harrison, *Cyber Risk Management: The Vital Role of Legal Management Professionals*, Legal Mgmt. (Oct. 2019), https://www.alanet.org/legal-management/2019/october/features/cyber-risk-management-the-vital-role-of-legal-management-professionals.

2. *See generally* Daniel Schwarcz, *Transparently Opaque: Understanding the Lack of Transparency in Insurance Consumer Protection*, 61 UCLA L. Rev. 394 (2014).

3. *Id.* at 409–13.

4. Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 Yale J.L. & Tech. 106, 119 (2019).

5. Anat Lior, *Insuring AI: The Role of Insurance in Artificial Intelligence Regulation*, 35 Harv. J.L. & Tech. 467, 478 (2022).

6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

7. Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 Denver L. Rev. 93, 111–12 (2020).

8. *Id.* at 113.

9. Brian Daigle & Mahnaz Khan, *The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities*, J. Int'l Com. & Econ., June 2020, at 1, 4.

10. Lilian Edwards, *Data Protection: Enter the General Data Protection Regulation*, *in* Law, Policy and the Internet (2018).

11. GDPR, *supra* note 6, at art. 83.

12. *Id.* at art. 4(1).

13. *Id.* at art. 3(1).

14. *See, e.g.*, *id.* at art. 23.

15. Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data Under the EU-US Data Privacy Framework, 2023 O.J. (L 231) 118.

16. *European Commission Gives EU-US Data Transfers Third Round at CJEU*, NOYB (July 10, 2023), https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

17. Caitlin Fennessy, *The EU-US Data Privacy Framework: A New Era for Data Transfers?*, IAPP (Oct. 7, 2022), https://iapp.org/news/a/the-eu-u-s-data-privacy-framework-a-new-era-for-data-transfers/.

18. Leah Shepherd, *EU Adopts New Standard Contractual Clauses for Data Transfers*, SHRM (July 28, 2021), https://www.shrm.org/resourcesandtools/hr-topics/global-hr/pages/eu-standard-contractual-clauses-data-transfers.aspx.

19. Emily Linn, *A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement*, 50 Vand. J. Transnat'l L. 1311, 1322–23 (2017); Michael Cairo, *Synthetic Data and GDPR Compliance: How Artificial Intelligence Might Resolve the Privacy-Utility Tradeoff*, 28 J. Tech. L. & Pol'y 71, 93 (2023).

20. *See* GDPR, *supra* note 6, at art. 56.

21. Heleen Janssen et al., *Decentralized Data Processing: Personal Data Stores and the GDPR*, 10 Int'l Data Priv. L. 356, 364–65 (2020).

22. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

23. 20 U.S.C. § 1232g.

24. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.

25. Brian Fung, *US Lawmakers Unveil a Plan to Give All Americans a Right to Online Privacy*, CNN (Apr. 8, 2024), https://www.cnn.com/2024/04/08/tech/online-privacy-bill/index.html.

26. *Id.*

27. Press Release, U.S. Senate Comm. on Com., Sci. & Transp., Committee Chairs Cantwell, McMorris Rodgers Unveil Historic Draft Comprehensive Data Privacy Legislation (Apr. 7, 2024), https://www.commerce.senate.gov/2024/4/

committee-chairs-cantwell-mcmorris-rodgers-unveil-historic-draft-comprehensive-data-privacy-legislation.

[28] *Id.*

[29] H.R. 8818, 118th Cong., 2d Sess. (2024).

[30] Cristiano Lima-Strong, *Lawmakers Unveil Sprawling Plan to Expand Online Privacy Protections*, Wash. Post (Apr. 7, 2024), https://www.washingtonpost.com/technology/2024/04/07/congress-privacy-deal-cantwell-rodgers/.

[31] H.R. 8818, § 117(a).

[32] *Id.* § 117(d).

[33] *Id.* § 101(53).

[34] *Id.* §§ 115–117.

[35] *Id.* § 101(13)(C)(iii), (51).

[36] Alexandra Kelley, *House Pivots on Data Privacy Bill, Removing Algorithmic Discrimination Coverage*, Nextgov/FCW (June 25, 2024), https://www.nextgov.com/digital-government/2024/06/house-pivots-data-privacy-bill-removing-algorithmic-discrimination-coverage/397618/.

[37] *Id.*

[38] Hunton Andrews Kurth, *American Privacy Rights Act Advances with Significant Revisions*, Nat'l L. Rev. (June 11, 2024), https://natlawreview.com/article/american-privacy-rights-act-advances-significant-revisions.

[39] Dell Cameron, *Surprise! The Latest "Comprehensive" US Privacy Bill Is Doomed*, Wired (June 27, 2024), https://www.wired.com/story/apra-privacy-bill-doomed/.

[40] Rebecca Klar, *Data Privacy Bill Markup Canceled After House Leadership Opposition*, The Hill (June 27, 2024), https://thehill.com/homenews/house/4742987-data-privacy-bill-markup-cancelled-after-house-leadership-opposition/.

[41] *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy*, White House (Mar. 2, 2023), https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

[42] Harry Coker, Jr., *One Year In: The President's National Cybersecurity Strategy Is Driving Change and Protecting the Nation*, White House (Mar. 4, 2024), https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/03/04/national-cybersecurity-strategy-one-year/.

[43] *Id.*

[44] *Fact Sheet: Biden-Harris Administration Releases Version 2 of the National Cybersecurity Strategy Implementation Plan*, White House (May 7, 2024), https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/05/07/fact-sheet-ncsip-version-2/.

[45] *Id.*

[46] Exec. Order No. 14306, Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144, 90 Fed. Reg. 24723 (June 11, 2025).

[47] *Id.*

[48] David S. Rubenstein, *Acquiring Ethical AI*, 73 Fla. L. Rev. 747, 787–88 (2021).

[49] *Id.*

[50] Press Release, U.S. Sec. & Exch. Comm'n, SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (July 26, 2023), https://www.sec.gov/newsroom/press-releases/2023-139.

[51] *Id.*

[52] *Id.*

[53] Pub. L. No. 117-103, div. Y, 136 Stat. 49, 1038.

[54] *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, Cybersecurity & Infrastructure Sec. Agency, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia (last visited Nov. 24, 2025).

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] Ins. Consumer Priv. Prot. Model L. #674 (Nat'l Ass'n of Ins. Comm'rs 2023), https://content.naic.org/sites/default/files/inline-files/Exposure%20Draft-Consumer%20Privacy%20Protection%20Model%20Law%20%23674%201-31-23.pdf.

[59] *Id.*

[60] *NAIC's Draft Revisions to Protect Consumer Privacy in Model Law 672*, JD Supra (Sep. 24, 2024), https://www.jdsupra.com/legalnews/naic-s-draft-revisions-to-protect-5890594/.

[61] Ins. Data Sec. Model L. (Nat'l Ass'n of Ins. Comm'rs 2017), https://content.naic.org/sites/default/files/model-law-668.pdf.

[62] *Id.*

[63] *Id.* § 4(E).

[64] *Id.* § 4(C)(5).

[65] *Id.* § 6(A).

[66] *Id.* § 6(B).

[67] *Insurance Data Security Model Law*, Nat'l Ass'n of Ins. Comm'rs (Summer 2025), https://content.naic.org/sites/default/files/model-law-state-page-668.pdf.

[68] *Id.*