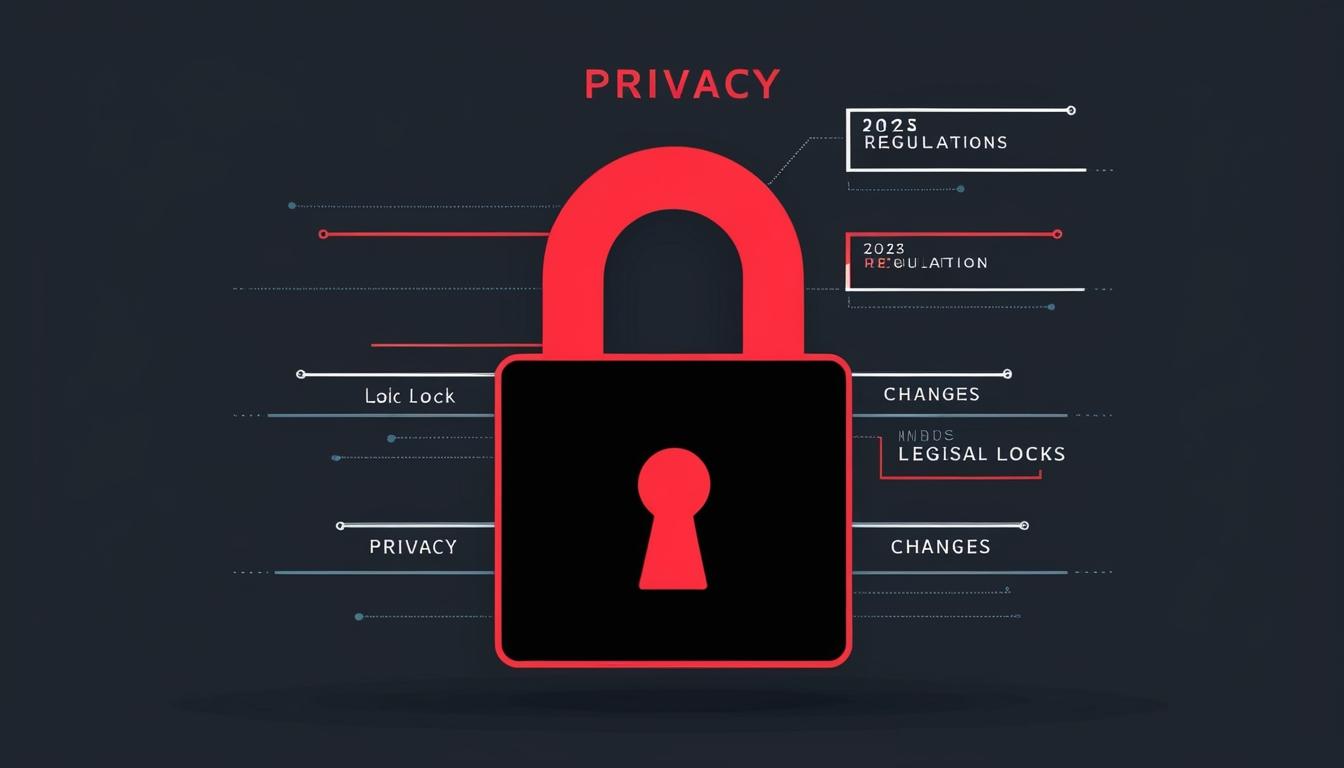
# The future of privacy and cybersecurity law in 2025



The landscape of privacy and cybersecurity law is poised for significant developments as the new Congress convenes on January 3, 2025, alongside a new administration set to begin on January 20, 2025. As states reconvene in early January, the first half of 2025 is anticipated to feature a wave of new legislation and regulatory activities, particularly concerning privacy laws and cybersecurity measures.

There are currently 20 general state privacy laws in existence across the United States. Among these is the Florida Digital Bill of Rights, which has set a revenue threshold of one billion dollars for compliance. New privacy laws in Delaware, Iowa, Nebraska, and New Hampshire came into effect on January 1, 2025, while the New Jersey Data Privacy Act is slated to follow on January 15, 2025. Additional laws from Tennessee, Minnesota, and Maryland are expected to come into force in the latter half of the year. Businesses may soon receive letters from state regulators emphasising the need to update their privacy notices in line with the new regulations.

The existing privacy frameworks continue to evolve, particularly with changes to the California Consumer Privacy Act (CCPA). The formal comment period on proposed updates to the CCPA, including regulations for cybersecurity audits and automated decision-making technology, is set to end on January 14, 2025. However, the path for federal legislative relief from the multitude of state privacy laws appears unlikely. Both the American Privacy Rights Act of 2024 and the American Data Privacy and Protection Act (2022) have failed to progress, with key points of contention centring around preemption and federal authority.

In December 2024, President-elect Donald Trump announced plans to elevate Andrew Ferguson, the current Commissioner, to the position of chair at the Federal Trade Commission (FTC). Ferguson has notably articulated that the FTC Act cannot be regarded as a comprehensive privacy law, stating in a recent statement that “Comprehensive privacy legislation involves difficult choices and expensive tradeoffs. Congress alone can make those choices and tradeoffs.” The anticipated changes in leadership at the FTC, moving away from the current Chair Lina Khan, suggest that new rules regarding commercial surveillance and data security might not materialise as a result of the 2022 Advance Notice on Proposed Rulemaking.

Recent actions by the California Privacy Protection Agency (CPPA) include the announcement of its first settlements with four data brokers that failed to register with state regulations. Both California and Vermont are enforcing data broker registration requirements as of this month, with Texas and Oregon establishing similar measures within specified timeframes. The CPPA has also released advisory opinions advising on data minimisation practices and the necessity for accessible user interfaces regarding privacy choices.

The topic of biometrics is emerging as a significant regulatory focus at both federal and state levels. A pertinent amendment to the Colorado Privacy Act (CPA) concerning biometrics is set to take effect on July 1, 2025. Unlike the CPA's general stipulations, this amendment will apply to employees.

Healthcare cybersecurity is also under scrutiny, with reports logged showing an increase in security incidents involving unsecured protected health information; 575 incidents affecting 500 or more individuals were recorded in 2024, compared to 265 in 2023. The Office of Civil Rights at the Department of Health and Human Services (HHS) has issued a Notice of Proposed Rulemaking aimed at modifying the HIPAA Security Rule, and further healthcare cybersecurity legislation is anticipated in 2025.

Over in Europe, the newly enacted AI Act highlights the first comprehensive regulation of artificial intelligence, establishing a risk-based framework that categorizes AI systems based on their potential for harm and imposes stringent requirements on those deemed high-risk. Furthermore, the European Data Protection Board has published its opinion on AI-related data processing, confirming that legitimate interest can serve as a basis for processing personal data.

As 2025 approaches, businesses must focus on developing privacy policies, creating user-friendly consent mechanisms, and establishing efficient systems for handling consumer requests. With state privacy laws and emerging regulations surrounding AI and biometrics gaining traction, it is essential for businesses to prioritise foundational compliance measures. This includes data privacy and cybersecurity risk assessments, crafting data processing agreements, and ensuring compliant practices in automated decision-making technologies. By addressing these initial requirements, companies can better navigate the intricate and evolving landscape of privacy and cybersecurity regulations.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.osano.com/articles/privacy-laws-2025> - Corroborates the new state privacy laws coming into effect in 2025, including those in Delaware, Iowa, Nebraska, New Hampshire, New Jersey, Tennessee, Minnesota, and Maryland.
2. <https://www.globalprivacywatch.com/2025/01/a-new-year-and-new-compliance-requirements-additional-state-privacy-laws-take-effect-in-2025/> - Provides details on the effective dates and applicability thresholds of the new state privacy laws in 2025.
3. <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/> - Tracks comprehensive US state privacy bills and their effective dates, including those mentioned for 2025.
4. <https://www.osano.com/articles/privacy-laws-2025> - Mentions the revenue thresholds and consumer data processing requirements for the new state privacy laws.
5. <https://www.globalprivacywatch.com/2025/01/a-new-year-and-new-compliance-requirements-additional-state-privacy-laws-take-effect-in-2025/> - Explains the specific requirements and restrictions of the Maryland Online Data Privacy Act, including data collection limitations.
6. <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/> - Details the upcoming changes and effective dates for various state privacy laws, including Colorado's biometrics amendment.
7. <https://www.osano.com/articles/privacy-laws-2025> - Highlights the importance of businesses updating their privacy notices in line with the new state regulations.
8. <https://www.globalprivacywatch.com/2025/01/a-new-year-and-new-compliance-requirements-additional-state-privacy-laws-take-effect-in-2025/> - Discusses the evolving privacy frameworks, including updates to the California Consumer Privacy Act (CCPA).
9. <https://www.iapp.org/news/a/article/california-privacy-protection-agency-announces-first-settlements-with-data-brokers/> - Corroborates the California Privacy Protection Agency's actions, including settlements with data brokers and advisory opinions on data minimisation practices.
10. <https://www.hhs.gov/about/news/2024/12/notice-proposed-rulemaking-hipaa-security-rule.html> - Supports the information on the Notice of Proposed Rulemaking aimed at modifying the HIPAA Security Rule by the Office of Civil Rights at HHS.
11. <https://www.lexblog.com/2025/01/07/data-privacy-and-cybersecurity-look-ahead-first-half-of-2025/> - Please view link - unable to able to access data