U.S. Privacy Regulations

Andrew Kingman: The Lobbyist Striking Balance in Privacy Policy

July 2025

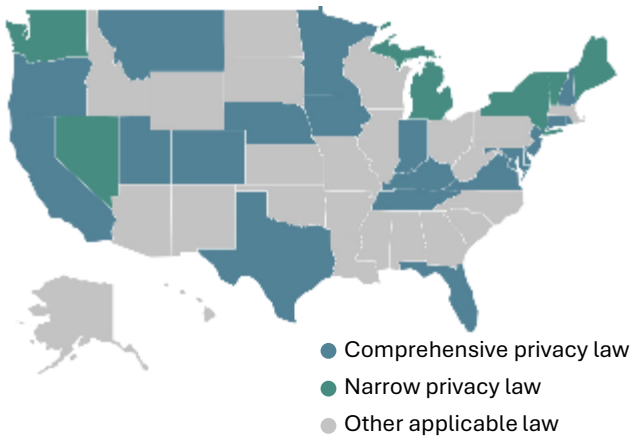
WASHINGTON | CORE

Andrew Kingman has been a central player in the debates over the enactment of privacy laws in the U.S. In the absence of privacy laws at the federal level, individual U.S. states are stepping in to regulate. California's pioneering consumer privacy law was widely expected to be emulated by other states, but other states have opted to go their own way, and Kingman has played a crucial role in encouraging state officials to pursue a model with more operational feasibility. We asked Mr. Kingman, who is a leading privacy lawyer and tech lobbyist, about privacy protection in the U.S. and the outlook for the future.

20 States Have Enacted Privacy Laws

According to Kingman, the State Privacy and Security Coalition (SPSC) has played a central role in shaping what has become the default model for state-level privacy laws. The SPSC is a multi-industry organization representing a wide range of sectors, from tech giants like Amazon, Google, and Meta to telecom firms like AT&T and Comcast, major retailers like Target, and even automakers like General Motors.

Kingman serves as an advisor to state policymakers seeking to strengthen privacy and cybersecurity laws and regulations. In this capacity, he has spent the past decade advising state legislators and regulators on the development of data privacy legislation in their respective state legislatures.



As of June 2025, 20 U.S. states have enacted privacy laws, collectively covering more than 140 million people, and the number is expected to grow. A "default national standard" is emerging through state laws, as it has become common practice for states to discuss and incorporate each other's ideas when attempting to legislate.

Private Right of Action: "It's the Lawyers Who Profit"

One of the most contentious issues in state privacy law is the right of individuals to sue companies for privacy violations, or the Private Right of Action (PRA). While California law explicitly includes aspects of the PRA for certain types of data breaches, other states have debated whether to include it. Kingman has strongly advised states against adopting the PRA, calling it a significant pitfall.

The PRA provision opens the door for consumers to file class action lawsuits over privacy, which Kingman argues would do more harm than good. He says that the majority of the benefits will accrue to consumers' attorneys, rather than to the consumers themselves. He also noted that if privacy litigation becomes available in one state, it could open the floodgates for businesses to be sued in all 50 states, making it impossible for businesses to function. Out of the 20 state privacy laws, only California's includes a broad PRA clause, and even California limits its use.

Instead of PRA, Kingman promotes the concept of a "cure" period

This would give companies a 30–60-day window to correct privacy violations before penalties are imposed. In California's experience, 75% of businesses that received cure notices fixed the compliance issue right away, demonstrating its effectiveness. However, consumer advocates argue that cure periods, while reducing legal uncertainty for businesses, may delay meaningful recourse for consumers. Some consumer advocates question whether companies would have incentives to fully comply with privacy protections without the potential for civil enforcement by individuals.

Vermont, the Snowy State: Ski Resorts and the Necessity of Data Collection

Kingman also emphasizes that with states enforcing privacy protection in the absence of federal legislation, it is important to create privacy laws that are appropriate to each state. For example, Vermont, where the ski business is thriving, needs data governance that meets the needs of the local industry. Ski resorts use contactless cards (RFID) for lift access and to collect customer information. It is important to use that data to develop digital advertising and attract repeat customers. Applying strict privacy regulations to such efforts would frustrate the marketing strategy, which would be a major blow to the local industry. Kingman and his colleagues lobbied a wide range of stakeholders early on, including business leaders, the state attorney general, and civic groups, to find a solution to Vermont's privacy law. Organized lobbying groups have also been mobilized. For example, a lobbying group called the Connected Commerce Council (3C), launched a major Facebook and Instagram campaign shortly after the strict bill was introduced. The campaign explained that the bill would make it "harder and more

expensive to know and communicate with customers, advertise online, and use powerful analytics from your advertising, e-commerce, and email marketing partners." In response, the governor decided that the original proposal, as written, would make people think that Vermont is hostile to businesses, leading him to veto the bill. A new bill, a compromise between the two sides, is currently being discussed, with the state Senate passing a version of the framework that has passed in other New England states. The House's version plans to regulate "content-linked advertising" based on the content of web pages, and "first-party advertising" based on customer data collected and held by companies themselves would be allowed under certain circumstances. Regarding consumer protection, "targeted advertising" aimed at user groups with specific attributes and behaviors, as indicated by browsing history, was prohibited, and a more explicit opt-out feature was included. The Vermont example illustrates the importance of carefully crafting laws in a flexible manner, taking into account both consumer protection and local business interests.

Automatic Profiling and Consumer Rights in Minnesota

Andrew Kingman testifying before the Joint Committee on Advanced Information Technology, Internet and Cybersecurity

While each state has its own complexities, the comprehensive consumer data privacy law passed in Minnesota in June 2024 is particularly unique. Amongst the privacy bill provisions that were debated were a requirement that businesses document compliance with privacy requirements, and a consumer right to challenge the results of automated profiling, the potentially discriminatory practice of using AI algorithms to typify and "automatically profile " consumers.

Both are unprecedented provisions that do not exist in other state privacy laws, but the bill's sponsor, Rep. Steve Elkins, was adamant that they be made requirements. After working together in good faith, the two sides reached an agreement to incorporate the provisions in a form that could be implemented with as little burden as possible. Specifically, if automated profiling has legal or serious consequences, consumers have the right to dispute those consequences, to know why they reached those consequences, and to be told, if possible, how they could have reached a different conclusion. Additionally, consumers have the right to access and correct their personal information and the right to have their profile reconstructed with the correct information. Although other states (e.g., Montana and Nebraska) also provide automatic profiling opt-out rights, Minnesota consumers won privacy protections that went one step further than that. The bill, a win-win for consumer protection and practical legislation, was ultimately passed.

Avoiding a Regulatory Minefield

Kingman warns that without federal legislation; the 50 states could end up being a regulatory minefield of disparate privacy laws. To reduce the burden on companies, he advocates for unifying core elements such as the scope of sensitive data, data minimization, data sales rules, and AI and profiling guidelines across the states.

The U.S. approach to privacy regulation is often framed as a balance between privacy protection, user experience, and individual choice. Though it drew initial inspiration from the EU's General Data Protection Regulation (GDPR), it has taken a notably different path. Unlike Europe, which accepts some consumer inconvenience in exchange for stronger protections, the U.S. prioritizes usability and innovation. While this benefits businesses, consumer advocates argue it can come at the expense of robust consumer safeguards.

Kingman emphasizes that U.S. state privacy laws are often a simplified version of the GDPR, meaning that most global companies that comply with the GDPR can also be in compliance with U.S. rules, However, the reverse is not always true, which raises concerns that American consumers may not enjoy the same rights available to EU citizens.

Kingman said that challenging situation of each state having its own regulatory approach is giving way to a convergence toward a "reasonable middle ground." As states align, federal legislation may eventually follow. Given the pace of technological change, he argues that a flexible, adaptive approach, rather than strict governance from the outset, may be the most practical path for the U.S.

Andrew Kingman is an attorney and president of the law firm Mariner Strategies LLC. He is also counsel to the State Privacy and Security Coalition (SPSC). He has expertise in privacy, technology, and cybersecurity law and has played a central role in the development of state-level privacy legislation throughout the United States. As counsel to the State Privacy & Security Coalition, he has advocated for workable privacy laws on behalf of major economic sectors such as technology, retail, telecom, and automobiles.