



August 25, 2025

# A Year In Data Privacy Is A Lifetime, So Your ‘New’ Compliance Policy May Already Be Outdated

by Gary Kibel

Everything seems to get better and last longer. Remember when it was recommended to change your oil every 3,000 miles? Now it is 5,000 miles. Remember when milk used to go sour in the fridge in a few days? Now it will make it through the weekend.

However, as the realm of privacy law advances, compliance is becoming more complicated. Remember when you could update your privacy disclosures and be in good shape for a few years? Well, those days are long gone.

New privacy laws are being enacted on the state level at breakneck speed, and lawmakers keep moving the goalposts. As a result, even if you updated your privacy policy and other aspects of your compliance program last year, it may already be outdated.

Here's how the latest state privacy laws are changing the compliance game.

## Fifty states, fifty standards

In July alone, new comprehensive, wide-ranging consumer privacy laws in Tennessee and Minnesota took effect. This brings the number of states with comprehensive consumer privacy laws to 15. Four more states – Maryland, Rhode Island, Kentucky and Indiana – plan to enter the fray by next January.

Other states have enacted dozens of laws focused on children's data, geolocation data, biometrics, data brokers and more. As can be expected, these laws do not mirror one another, so the disconnects continue to grow.

The Tennessee Information Protection Act (TIPA) requires companies to maintain and comply with a written privacy program that reasonably conforms to the National Institute of Standards and Technology (NIST) privacy framework if they want an affirmative defense to a violation of the TIPA.

Meanwhile, the Minnesota Consumer Data Privacy Act requires controllers to name a chief privacy officer or other individual (such as a data protection officer) with primary responsibility for directing policies and procedures implemented to comply with the law. Controllers in Minnesota must also affirmatively notify consumers of any material change to the controller's privacy policy or personal data practices and, for

previously collected personal data, provide a reasonable opportunity for consumers to withdraw consent to any materially different processing.

Perhaps the most significant upcoming law is the Maryland Online Data Privacy Act, which takes effect this October. The industry has [previously been warned](#) about how significant that law will be for the digital media ecosystem; it's considered one of the strictest state privacy laws to date, introducing broad restrictions on data collection, targeted advertising and selling of sensitive data that go beyond existing US privacy frameworks.

## Different regulators, different rules

While compliance is challenging, the next phase – enforcement – is starting to pick up steam. Regulators in California, Connecticut, Texas and other states are reaching out to businesses and bringing enforcement actions. Each state regulator is solely focused on the requirements of their own state's law and does not care if a business is complying with other states while missing unique aspects of their state.

As the industry waits, begs and pleads for Congress to bring some sanity to this issue by passing a federal comprehensive consumer privacy law that preempts all of the state laws, businesses must focus on compliance.

Privacy compliance is not a one-and-done exercise; it is a nonstop, ever-changing environment that requires commitment in an organization from the top down. The bottom line: The US privacy landscape is getting more fragmented, more aggressive and more enforcement-driven. Maryland's law may be the most restrictive yet, but it won't be the last.

Organizations need to stop treating privacy as a periodic update and start treating it as an active, ongoing capability, built to flex with changing laws, user expectations and real operational risk.



**Gary Kibel** is a partner in the Privacy, Technology + Data Security Practice Group of Davis+Gilbert LLP. He may be reached at [gkibel@dglaw.com](mailto:gkibel@dglaw.com) or 212 468 4918.

