DAVIS + GILBERT

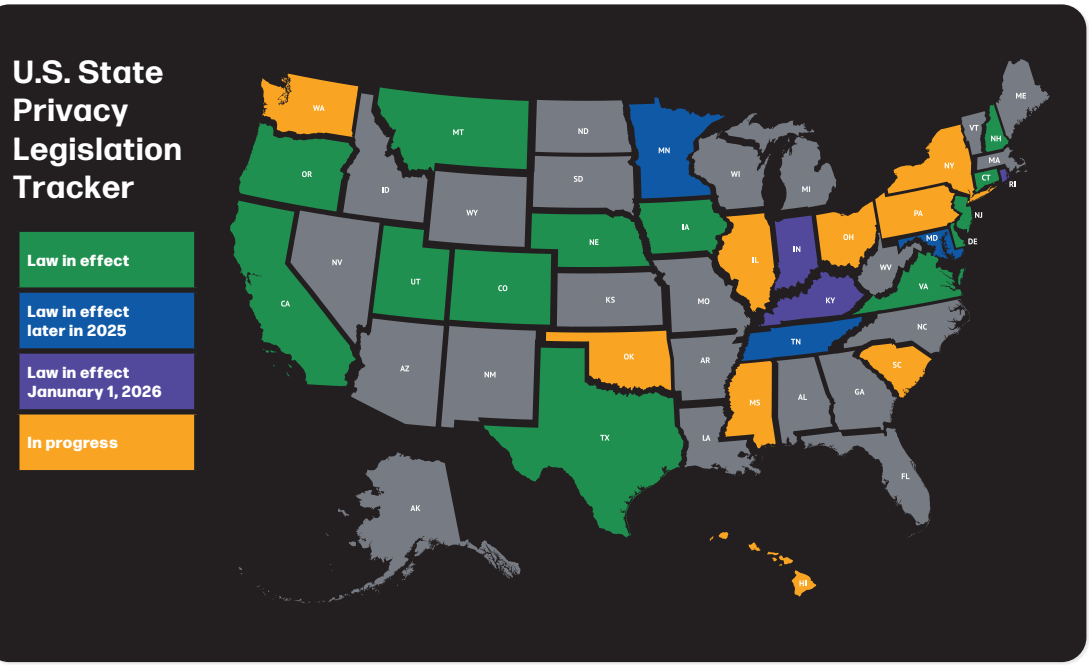
Privacy Compliance Obligations TO GROW More Complex

Privacy law has become one of the fastest-evolving areas of regulation in the United States, with significant implications for businesses across industries.

The emergence of 19 state comprehensive privacy laws, increased focus on sensitive data, and heightened scrutiny of children's data collection practices are reshaping compliance obligations. With the absence of a comprehensive federal privacy law in the United States, businesses are left to navigate compliance across different state laws – with rules that vary from state to state depending on how a business is collecting and using data, its size, and more.

At the same time, federal enforcement efforts are unclear, while state regulators are ramping up enforcement efforts in certain areas and creative class-action lawsuits breathe new life into decades-old privacy laws. As privacy challenges grow more complex, businesses must stay ahead of these developments to navigate the shifting legal landscape and mitigate risks effectively.

U.S. State Privacy Legislation Tracker



Expanding Landscape: Patchwork of 19 U.S. State Privacy Laws

Shifting Strategies: Age-Appropriate Design Codes & Child Data Laws Reshaping Advertising Practices

Litigation Surge: Class Actions Piggyback on Decades-Old Privacy Laws

Sensitive Data Under the Microscope: State Privacy Law Focus & FTC Enforcement Trends

Rising Scrutiny: Federal & State Enforcement Expected to Intensify in 2025

DAVIS GILBERT

Expanding Landscape: Patchwork of 19 U.S. State Privacy Laws

By: Richard Eisert, Gary Kibel & Zachary Klein

Richard Eisert

Partner
212 468 4863
reisert@dglaw.com

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Zachary Klein

Associate
212 237 1495
zklein@dglaw.com

U.S. state lawmakers continue to roll out new privacy laws at a relentless pace. Just a few years ago there was only one – the *California Consumer Privacy Act* (*CCPA*). Now, 19 comprehensive privacy laws have been enacted.

States with Laws Currently in Effect (13)

California	Montana	Texas
Colorado	Nebraska	Utah
Connecticut	New Hampshire	Virginia
Delaware	New Jersey	
Iowa	Oregon	

States with Law Coming into Force Later in 2025 (3)

Maryland	Minnesota	Tennessee

States with laws to become effective on January 1, 2026 (3)

Indiana	Kentucky	Rhode Island

This rapid expansion signals a patchwork of regulations that businesses must navigate to ensure compliance. As these laws continue to evolve and overlap, organizations face increasing challenges in harmonizing their data protection practices across jurisdictions.

Nuances Complicating Compliance

Although these laws (thankfully) share more in common than not, distinguishing features complicate compliance efforts. Further, no single state has the strictest standard, so businesses do not have the luxury of just complying with the highest standard available. Full compliance involves considering all of the state laws.

Below are some of the latest emerging critical differences businesses should be aware of:

Children's Data Protections

On top of the federal *Children's Online Privacy Protection Act* (*COPPA*) rules for processing the data of children under 13, several states require businesses to obtain opt-in consent from 13- to 15 year-old consumers to sell their personal data or use it for targeted advertising. However, in 2025, several states will push the age threshold even higher, as New Jersey and Minnesota have raised the age threshold to include minors between 13 and 16, and Delaware to 17 years of age. Maryland will institute an outright ban on data sales and targeted advertising to users under 18.

Applicability Thresholds

In order for their laws to apply, the majority of states consider threshold criteria such as a company's annual revenue and/or the number of individuals' data processed. However, Texas and Nebraska rely on a completely different standard, judging whether organizations are "small businesses" as defined by the U.S. Small Business Administration. Companies previously exempt from other state laws may need to comply with the laws in Texas and Nebraska if they don't qualify as "small businesses."

Expanded Right of Access

Every state comprehensive privacy law provides consumers with a right of access that requires businesses to confirm whether they are processing the consumer's personal data and to grant access to that data. Oregon and Minnesota, however, go further by requiring controllers to provide a list of the specific third parties with whom they have shared personal data. Delaware has a less granular requirement that controllers provide a list of the categories of third parties (not specific entities) to which the controller has disclosed the consumer's personal data.

State Agency Rulemaking Authority

Until recently, California and Colorado were the only states to offer rulemaking authority to their respective enforcement agencies. However, New Jersey and New Hampshire will now grant similar powers to their own state agencies under their privacy laws. If California's and Colorado's enacted regulations are any guide, businesses can expect nuanced rules that clarify and build heavily upon New Jersey's and New Hampshire's statutory requirements.

Looking Ahead

Navigating compliance across multiple state privacy laws continues to be a challenging but essential task for businesses. Therefore, companies should regularly revisit their privacy practices to ensure their compliance efforts are up to date.

DAVIS GILBERT

Shifting Strategies: Age-Appropriate Design Codes & Child Data Laws Reshaping Advertising Practices

By: Allison Fitzpatrick, Gary Kibel & Zachary Klein

Allison Fitzpatrick

Partner
212 468 4866
aftizpatrick@dglaw.com

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Zachary Klein

Associate
212 237 1495
zklein@dglaw.com

While Democrats and Republicans do not agree on much these days, they do agree on strengthening children's online privacy protections. The bipartisan push has resulted in significant legislative developments at both the federal and state levels.

Federal Legislative Actions

The Senate overwhelmingly passed two major bills over the summer of 2024:

- The *Children and Teens' Online Privacy Protection Act* (*COPPA 2.0*), which bans online companies from collecting personal information from users under 17 years old without their consent, as well as bans targeted advertising to children and teens.
- And the *Kids Online Safety Act* (*KOSA*), which requires online platforms to establish a "duty of care," activate the most protective settings for kids by default, and provide minors with options to protect their information, disable addictive product features and opt-out of personalized algorithmic recommendations.
- Late last year the FTC issued rules amending COPPA which impose new requirements to collect and process personal information from children under 13, including regarding consent and data retention.

State-Level Developments

While federal laws take shape, states are also advancing their own child data protection laws. California, Connecticut, Oregon, Montana and New Hampshire require businesses to obtain opt-in consent from 13 to 15-year-old consumers to sell their personal data or use it for targeted advertising. In 2025, several states will push the age threshold even higher:

- New Jersey and Minnesota have expanded the scope of this requirement to include minors between 13 and 16.

- Delaware's law extends to consumers 17 years of age.
- Maryland takes the most restrictive approach and will institute an outright ban on data sales and targeted advertising to users under 18 when its law takes effect in October.

Despite the Ninth Circuit's decision to uphold much of a lower court's injunction of the ***California Age-Appropriate Design Code***, a number of states have advanced similar legislation:

- The *Maryland Age Appropriate Design Code*, which applies to online products "reasonably likely to be accessed by children," took effect October 1, 2024, and mirrors a number of elements of ***KOSA***, including obligations for companies that process children's data to act in the "best interests of children."
- Michigan and Pennsylvania are currently considering age-appropriate design codes of their own.
- New York passed both the *Child Data Protection Act and Stop Addictive Feeds Exploitation (SAFE) for Kids Act*, which protect children and teens under 18 years of age. These laws regulate the collection, sale, and usage of a minor's personal information, including prohibiting social media companies from showing addictive, algorithmic feeds and overnight push notifications to minors.

Looking Ahead

It is very likely that we will see more enforcement in this area, as states are increasing their enforcement staffs and the FTC will likely continue to focus on children's data given the bipartisan support.

DAVIS + GILBERT

Litigation Surge: Class Actions Piggyback on Decades-Old Privacy Laws

By: Marc Rachman & Sarah Benowich

Marc Rachman

Partner, Litigation + Dispute Resolution
212 468 4890
mrachman@dglaw.com

Sarah Benowich

Associate, Litigation + Dispute Resolution
212 468 4991
sbenowich@dglaw.com

Plaintiffs' lawyers have made an industry of bootstrapping decades old anti-wiretapping laws into class actions, taking advantage of the right to recover statutory damages (and attorneys' fees) provisions and murky court decisions denying motions to dismiss.

California's Invasion of Privacy Act (*CIPA*) has remained a focal point. Originally designed to prevent unwanted eavesdropping on telephone calls, *CIPA* has become a hotbed for class actions against technologies that are at the heart of most website functionality, including the cookies, pixels, chatbots and other tools that can track users' online activity. These technologies, designed to enhance consumers' interactions with websites, generate analytics, deliver targeted advertising and create consumer profiles, are frequent targets of litigation.

Given the ubiquity of tracking technologies and enough precedent permitting these claims to proceed, we expect these actions to only increase in 2025, even as the targets of these suits try to hone their privacy policies, terms of use and consent mechanisms to provide a shield against such claims.

Key Types of CIPA Claims

CIPA claims generally fall into two categories: (1) under Section 631(a)'s prohibition on wiretapping; and (2) increasingly under Section 638.51's prohibition on the installation and use of a pen register or trap and trace device, so-called "pen register" claims.

Wiretapping Claims

CIPA Section 631(a) generally prohibits "wiretapping," which historically concerned unwanted eavesdropping on telephone calls. Plaintiffs have even parlayed Section 631's prohibition against "aiding and abetting" wiretapping to file claims against software development kits (SDKs) for allegedly surreptitiously tracking or recording consumer communications and interactions with the websites in which the SDKs are embedded.

A user's consent or authorization to such interception may be a defense to wiretapping claims, but not all courts will take judicial notice of external privacy policies, terms of use, or consent flows. This means that some cases may survive a motion to dismiss – despite ironclad privacy policies, terms of use and consent mechanisms.

Pen Register or Trap and Trace Device Claims

A new wave of claims draws on Section 638.51, which prohibits the "install[ation] or use [of] a pen register or a trap and trace device without first obtaining a court order" or consent, in certain circumstances. ***CIPA*** defines a pen register as a device or process that records or decodes dialing, routing, addressing, or signaling information, but not the contents of a communication. In contrast, a "trap and trace" device is defined as functionally similar, but it records the incoming rather than outgoing numbers to a particular line.

While consent is a complete defense to ***CIPA*** wiretapping claims, courts are mixed as to whether consent defeats pen register claims. Some courts have limited the consent defense to those entities that qualify as providers of "electronic or wire communication service[s]." Still, we expect (and encourage) website, app, and software providers to continue to strengthen their privacy policies, terms of use, and consent flows to include very clear consent disclosures, choice of law provisions, class action waivers, and arbitration provisions.

Looking Ahead

Despite pre-dating the internet, class actions lodging ***CIPA*** claims against website operators, mobile app developers, and software providers are only expected to rise as courts ignore policy and practical arguments that ***CIPA*** should not apply to commonplace internet technologies.

DAVIS GILBERT

Sensitive Data Under the Microscope: State Privacy Law Focus & FTC Enforcement Trends

By: Gary Kibel

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Sensitive data has emerged as a focal point for both state lawmakers and federal regulators, who are prioritizing how businesses handle sensitive information such as health data, biometric identifiers, data from children and precise geolocation. The Federal Trade Commission (FTC) is taking an assertive stance, with recent enforcement actions demonstrating its commitment to addressing improper handling of sensitive information. Companies must remain vigilant, as noncompliance can result in significant legal and reputational risks.

Consumer Health Data

The past few years have seen the passage of multiple laws relating to consumer health data, particularly those in Connecticut, Nevada and Washington. The litigation impact of the ***Washington My Health My Data Act's*** (***MHMD***) private right of action has yet to be felt, but businesses are watching legal developments in this state closely.

In January 2025, New York state lawmakers passed the ***New York Health Information Privacy Act*** (***NYHIPA***), which shares many similarities with ***MHMD*** (including a private right of action) and adds new, stricter requirements not seen in the other three state laws. If signed, ***NYHIPA*** would create the broadest protections for consumer health data to date.

Children's & Teens' Data

State and federal efforts have also intensified regarding children's and teens' data. In 2024, the U.S. Senate passed the ***Children and Teens' Online Privacy Protection Act*** (***COPPA 2.0***) and the ***Kids Online Safety Act*** (***KOSA***), which aim to extend ***COPPA's*** protections to minors under 17 and introduce additional safeguards. As those bills are pending, in January 2025, the FTC issued rules amending the existing ***COPPA*** framework, imposing new requirements to collect and process personal information from children under 13.

Virginia, Colorado and Connecticut have amended their existing consumer data privacy laws to impose additional requirements for processing data of children under 13, while existing laws in Utah and Florida impose a range of requirements

for online platforms that provide an online service, product, game or feature likely to be predominantly accessed by children (i.e., social media). Additionally, Maryland enacted legislation to protect children and teens under 18 years of age, and New York signed into law its new *SAFE for Kids Act and Child Data Protection Act*.

Maryland's "Strictly Necessary" Standard

Maryland has taken a major new step in prohibiting the processing of sensitive data unless "strictly necessary" to provide or maintain a product or service requested by the consumer. This is a stricter standard than the opt-out, opt-in consent, and "limit the use" rights in other states, or the common standard that the processing of personal data generally be "reasonably necessary" in relation to disclosed purposes. However, the Maryland law is unclear as to how "strictly necessary" should be interpreted, which could create conflicts with other statutory provisions and cause compliance uncertainty.

FTC Enforcement Trends

The FTC has been particularly active in enforcement against practices relating to the collection and sale of location data that can be used to infer sensitive characteristics. Following recent settlements with Kochava, InMarket and X-Mode, in December 2024, the FTC issued orders against Mobilewalla, Inc. and Gravy Analytics Inc. based on their practices of collecting and selling raw location data that can be used to identify sensitive locations that consumers have visited. Mobilewalla, in particular, was alleged to have helped its clients target pregnant women, Hispanic churchgoers and members of the LGBTQIA+ community based on the locations that they had visited.

The FTC deemed these activities to constitute an unfair trade practice under the *FTC Act*, alleging in part that the collection and sale of consumer data, particularly data based on sensitive characteristics, "causes or is likely to cause substantial injury in the form of stigma, discrimination, physical violence, emotional distress, and other harms," and is not outweighed by a countervailing benefit to consumers or competition.

Looking Ahead

It remains to be seen whether the FTC's enforcement priorities will persist in light of the Commission's leadership changes in 2025.

DAVIS GILBERT

Rising Scrutiny: Federal & State Enforcement Expected to Intensify in 2025

By: Richard Eisert

Richard Eisert

Partner
212 468 4863
reisert@dglaw.com

While 2025 brings significant changes to the FTC, raising questions about the pace and scope of federal enforcement of privacy-related initiatives, the picture looks very different on the state level. As state privacy laws continue to multiply, an increasing number of regulators are bringing enforcement actions and issuing advisories, adding to concerns of companies trying to comply with this complex web of state requirements.

Based on recent enforcement trends, certain priorities for regulators in 2025 are already coming into focus.

Data Broker Laws

Enforcement of data broker laws will remain a focus of regulatory attention in 2025. On November 8, 2024, the California Privacy Protection Agency (CPPA) Board voted to adopt new regulations clarifying the ***Delete Act*** (which amends California's existing ***Data Broker Registration*** law) in key areas, including:

- regulation and information submission requirements,
- procedures for registration changes, and
- the threshold criteria for a company to be considered a data broker.

Following this, the CPPA announced settlements with two data brokers – Growbots, Inc. and UpLead – for failing to register and pay annual fees.

Sensitive Data

The processing of sensitive personal data without consent has been, and likely will remain, a key focus for state regulators. The FTC has taken action against companies collecting and selling raw location data that revealed information about a consumer's religion, sexuality and more.

State attorney generals, including in the State of Texas, have also engaged in several enforcement actions in this area focused on the collection of biometric

data without consent, collecting and selling personal information of children and teens, and collecting, using, and selling location data.

Dark Patterns

Dark patterns are not only a key priority for the FTC, but many states have also dialed in on protecting consumers from these deceptive practices when regulators believe they are being used by online services to mislead or trick their users.

- Last year, California announced dark patterns as an enforcement priority, releasing an enforcement advisory that provides guidance on how to avoid dark patterns, stating, "using clear and understandable language and offering consumers symmetrical choices avoids impairing and interfering with consumers' ability to make their choice."
- Other states, including Colorado and Connecticut, have also expressly restricted the use of dark patterns in acquiring consent.

Looking Ahead

While the FTC's new leadership considers their enforcement priorities, we can expect to see a rise in enforcement on the state level, particularly in the areas noted above.

Robert Chappell, an intern in the Advertising + Marketing and Privacy, Technology + Data Security groups at Davis+Gilbert, assisted with this alert.

Conclusion
Looking Ahead

As privacy laws continue to evolve and enforcement intensifies, businesses must adopt proactive compliance strategies.

By understanding state-specific nuances, prioritizing sensitive data protections, and preparing for increased litigation and regulatory enforcement risks, organizations can navigate this complex landscape and mitigate potential liabilities in 2025 and beyond.

Actionable Insights

1. Conduct data audits to understand a company's data collection and processing activities.
2. Consider whether to align privacy policies and practices with the most stringent requirements across applicable jurisdictions or to take a state by state approach.
3. Implement robust consent mechanisms for sensitive data collection.
4. Regularly review third-party relationships to ensure compliance with data-sharing requirements and put in place appropriate contractual terms, such as a Data Processing Agreement (DPA).
5. For children's data, strengthen consent flows and parental notification mechanisms.
6. Monitor enforcement trends as states indicate their priorities and ramp up resources in this area.
7. Proactively register with applicable state data broker registries where required.
8. Avoid dark patterns by providing clear, symmetrical choices for consumers.
9. Conduct privacy impact assessments to identify potential areas of exposure.
10. Regularly update terms of use and privacy disclosures to maintain compliance with new laws and industry trends.