Top 5 State Privacy Issues We're Monitoring This Year

Alysa Z. Hutnik, Alexander I. Schneider

January 9, 2024

The year ahead promises to be busy on the state privacy front. As we've covered on this blog, states are continuing to fill the gap at the federal level by implementing comprehensive state laws that guarantee consumer privacy rights and regulate data sales, targeted advertising, and sensitive data.

Now, more states than ever are jumping on the bandwagon with comprehensive privacy laws on the books in more than 25 percent of U.S. states and new legislative efforts underway in many other states. In 2024, new laws in Florida, Tennessee, Texas, and Oregon will take effect, joining laws already in effect in California, Colorado, Connecticut, Utah, and Virginia. Laws focused on consumer health data take effect in Washington and Nevada in March as well.

As we look ahead to 2024 activity, we're particularly monitoring for developments in the following five areas as the year unfolds:

1. ENFORCEMENT

- For the most part, state privacy law enforcement has taken place outside the public view in the form of informal inquiries, consumer complaints, and enforcement sweeps. Public enforcement actions in 2024 will no doubt garner attention and demonstrate the types of issues that enforcement agencies are initially prioritizing under the new privacy laws. We will be watching closely for public enforcement actions stemming from the slate of new state privacy laws that have taken effect over the last year.
- Since the California Consumer Privacy Act (CCPA) took effect on January 1, 2020, the only public state privacy enforcement action with monetary penalties was the California Attorney General's August 24, 2022 action against Sephora, which settled for $1.2 million. In the matter, the California AG clarified its view that Sephora's use of ad tech services involved a "sale" of personal information to these third parties. The case also placed a spotlight on the AG's requirement that companies recognize browser-level opt-out requests via opt-out preference signals.
- Other enforcement has been far more muted. The California AG published a series of enforcement summaries on its website in July 2021 and August 2022, which provide insight into how the agency interprets the CCPA. The California AG has also engaged in a variety of sweeps targeting opt-out preferences, employee privacy practices, and loyalty programs.
- The California Privacy Protection Agency (CPPA), for its part, is investigating connected vehicles and related technologies but has not announced a public enforcement action. However, a court order delayed enforcement of the agency's regulations until March 29, 2024, limiting the scope of the agency's potential enforcement activity until then.

- The Colorado AG announced enforcement of the Colorado Privacy Act by mailing letters to businesses to educate them about the new law, but has not announced any enforcement actions, and there is no public enforcement activity out of Connecticut or Virginia as of yet.
- **What to know:** Where a state regulator announces priorities or enforcement, it's worth paying attention to those developments and comparing to how your company's compliance matches up. If there are areas for improvement on such priority topics, it would be prudent to address sooner rather than later.

2. TECHNOLOGY

- We expect regulators, tech companies, and industry will continue to evaluate, adopt, and offer new technologies that facilitate compliance with privacy rights requests and privacy requirements in the coming year. These nascent technologies tie legal requirements to implementation (or monitoring for compliance) in a concrete way and are increasingly becoming the face of privacy laws.
- Seven of the new state privacy laws require businesses to recognize and respond to a universal opt-out preference signal typically sent from the consumer's browser. This signal allows a consumer to decide to opt out of the sale of their personal information for all websites, as opposed to making opt-out selections on a site-by-site basis.
- The Colorado AG led an effort to identify opt-out mechanisms that meet the requirements of the Colorado Privacy Act regulations. After review and public comment, the AG listed the Global Privacy Control (GPC) as a valid mechanism in Colorado. The GPC was also previously recognized by the California AG as a valid method of opting out of sales under CCPA.
- Another area to watch: the CPPA's new authority to develop a single mechanism that allows consumers to delete personal information held by data brokers registered with the state. Under SB 362 which passed the California legislature last year, the CPPA will be required to implement the new deletion mechanism by January 1, 2026, and in the intervening two years we expect to see the CPPA solicit feedback on, develop, and test this new deletion system.
- **What to know:** The new privacy legal landscape requires a lot of resources, manpower, technical support, education, and time. As the year proceeds, and the baseline of knowledge and expectations increases, regulators are likely to be less empathetic to arguments that compliance is difficult. If you have not already done so, it may be time to implement a privacy risk matrix to make the case on why you need more internal resources to support your company's compliance efforts (which has the added benefit of often supporting a durable data strategy).

3. CONSUMER HEALTH DATA

- On March 31, 2024, the majority of the substantive provisions of the Washington My Health My Data Act take effect. As we've written about on the blog, the new law is much broader than it may seem, and has significant implications for companies that collect or process the broadly-defined category of "consumer health data."
- In particular, the Washington law includes a path for private plaintiffs to seek damages under the Washington Consumer Protection Act for practices "covered" by the My Health My Data Act. The legislature included a declaration that the law addresses "matters vitally affecting the public interest" and that violations of the law constitute an "unfair or deceptive act in trade or

commerce," which are required elements under the Washington Consumer Protection Act. A plaintiff would still be required to establish injury caused by a violation of the My Health My Data Act to bring a claim. This new enforcement mechanism, along with state AG enforcement, could lead to a proliferation of privacy actions in Washington in the coming year.

- The law also reflects an increasing focus on the protection of sensitive data in state law. Whereas earlier iterations of state privacy laws traditionally focused on protecting social security numbers or financial account numbers, the new state privacy laws expand the definition of "sensitive" data to racial/ethnic origin, citizenship/immigration status, religious/philosophical beliefs, sex life, sexual orientation, biometric and genetic information, precise geolocation, and health information. This expanded set of sensitive elements is already requiring companies to reflect on the types of information that they collect, what information they share with other companies, and determine whether they need to modify business practices, including by collecting consent where necessary.

- **What to know:** If you have not already done so, it would be well worth the time to classify what data your company processes that meets the definition of health data or sensitive data under these laws and map whether your data processing activities are in line with the new restrictions and requirements. Unfortunately, there is not industry consensus on a taxonomy for such data but given how much rides on correct classifications, it would be prudent to be proactive here.

4. ACCOUNTABILITY

- Enforcement agencies are increasingly focused on promoting verifiable accountability for privacy practices, and we expect to see this trend continue throughout 2024.

- The most prominent example is the due diligence requirement in the new CCPA regulations that takes effect in March. The regulations incentivize businesses to conduct due diligence on any service providers, contractors, or third parties to which the business transfers or sells personal information to ensure these partners comply with CCPA requirements, stating that a business that "never enforces the terms of the contract" nor "exercises its rights to audit" might forgo a defense that the business believed its partner complied with the CCPA. It's a good reminder to account for a potential demonstration of one's compliance, including documenting due diligence and compliance check-ins during the life of the relationship.

- The CPPA is expected to conduct rulemaking into additional accountability measures: cybersecurity audit regulations, risk assessment regulations, and automated decision-making technology regulations. These draft regulations will create new assessments where businesses will be required to evaluate their privacy or security-related practices, document those practices, and in some cases provide transparency about such practices in the form of consumer-facing notices or regulatory filings. These details will be worked out over the course of 2024, with final regulations to take effect potentially as early as the first half of 2025.

- The Colorado, Connecticut, and Virginia laws already in effect require data protection assessments when engaging in certain data sales, targeted advertising, processing of sensitive data, or profiling activities. The AGs in these states may request these assessments as part of enforcement activities, and we'll continue to watch for any resulting public enforcement actions related to data protection assessments. Companies should consider how they're maintaining attorney-client privilege and protecting attorney work product versus what are non-privileged portions of the assessments that they'll need to produce in response to a regulator request (or

which could become targets in litigation discovery requests).

- California's new data broker law, SB 362, will also increase data broker accountability this year through mandatory disclosures that must be published by July 1, 2024. Data brokers will be required to compile and publish metrics about privacy requests received during the previous calendar year. Data brokers should also re-register with the CPPA's new data broker registry by January 31.

- **What to know:** As accountability obligations mount, companies can build out internal resources, knowledge, and infrastructure that will be needed to address new compliance documentation requirements. For example, consider incorporating due diligence and data protection assessment triggers into your new contract intake process to help incorporate privacy reviews into routine operations. Also, consider what steps may be necessary to ensure ongoing monitoring of partners for compliance.

5. FURTHER DISRUPTION

- So far, the state privacy laws have followed a predictable framework based on the consumer rights, accountability and transparency mechanisms, contract requirements, and regulation of data sales and targeted advertising first featured in the CCPA and refined in the Colorado, Connecticut, and Virginia privacy law templates.

- However, this framework that has persisted in 13 states is ripe for disruption. Already, states like Massachusetts, Maine, New Hampshire, and others have considered bills that take unique legislative approaches, some modeled on stalled federal legislation, that are drafted differently from existing state privacy laws.

- Harmonizing compliance with the current slate of 13 state privacy laws is possible in large part because legislatures have passed compatible legislation. Incompatible legislation would be a game-changer that would increase the challenge of compliance in a fractured legislative landscape.

- **What to know:** As we've seen in the last few years, the only constant in state privacy law is change. The ongoing challenge is building long-term privacy compliance infrastructure in the face of shifting legal requirements. We will continue to monitor and bring you the latest updates on new laws that take effect over the course of the coming year, to help you plan as much as possible for the road ahead.