Articles + Publications | October 2, 2024

The Rise of State Attorney General Privacy Enforcement

WRITTEN BY

Samuel E. "Gene" Fishel | Whitney L. Shephard

This article was originally published on October 2, 2024 in Westlaw Today. It is republished here with permission.

Gene Fishel and Whitney Shephard of Troutman Pepper highlight states with established privacy enforcement units, discuss the corresponding privacy acts in those states, and give recommendations for companies to mitigate risk and navigate a rapidly developing patchwork of regulatory standards.

Since the passage of the California Consumer Privacy Act (CCPA) in 2018, and in the absence of a comprehensive data privacy law at the federal level, states have increasingly sought to enact their own privacy legislation.

In 2023, seven states passed comprehensive consumer privacy laws, and six more have been enacted thus far in 2024, bringing the total to nineteen separate state laws and numerous other privacy-adjacent laws regulating, among other things, security of personal identifying information, consumer health data, and children's privacy.

While sharing many similarities in structure, the laws often diverge in their application both to businesses and to individuals, and in their enforcement mechanisms, which include dedicated privacy units, primarily in state attorney general (AG) offices, specifically tasked with developing guidance and ensuring compliance.

While it is important for companies to comply with all privacy laws in the states in which they operate, particular attention should be paid to those states that have established specialized units solely focused on enforcing their respective privacy acts, a trend that has accelerated in 2024.

A patchwork of state laws

The nineteen comprehensive state privacy laws enacted to date apply to the personal information of consumers, with the CCPA also extending to workers whose personal information is collected in their business capacities. "Personal information" is defined broadly across all the laws, with the CCPA, for example, defining it as any information that could be "reasonably associated" with or "reasonably linked" to an individual.

The laws universally grant consumers the right to access, correct, and delete such information, and to opt out of the sale and use of the data for targeted advertising and profiling. Each state law generally applies to all businesses and organizations that control or process the personal information of that state's residents, with most exempting nonprofit organizations except in Colorado, Oregon, and Delaware.

Further, the laws have applicability thresholds and data level exemptions which are not uniform between them and require careful analysis as to whether they subject an organization to their requirements.

For example, Texas's law, unlike other state laws, does not have gross revenue or volume of personal information processing thresholds to apply, but does note that it does not extend to "small businesses." Most state privacy laws provide an entity-level exemption for organizations regulated by the Gramm-Leach-Bliley Act (GLBA), except for Oregon and California.

Similarly, all comprehensive state privacy laws provide an entity-level exemption for organizations regulated by the Health Insurance Portability and Accountability Act (HIPAA) except for California, Colorado, Oregon, and Delaware, which only exempts HIPAA-related data and not the entity itself. These variances reinforce the importance for organizations to evaluate the data they control or process to determine potential exposure under these laws.

Most of the comprehensive laws also contain cybersecurity components that mandate businesses implement "reasonable" data security measures, supervise their vendors and service providers through specific contractual provisions, minimize the amount of personal information they collect, and conduct data protection assessments for potentially high-risk data processing.

Every law also requires businesses to disclose their privacy practices to consumers, and most require affirmative consent to process "sensitive" personal information, which includes child-related, healthcare, religious, or political data, among other types. While some states, such as California and Colorado, have promulgated detailed regulations to guide businesses in their compliance, most have not.

For many organizations that maintain a comprehensive privacy program, simply implementing one will not alleviate the need to address the permutations among these laws, including analyzing each law for specific requirements and exemptions that may apply to their industry sector and individual business practices.

Importantly, while many state laws were passed with "cure" periods, which allow organizations to remediate alleged violations of the law within a specified period, around half of these cure periods expire one year after the laws take effect, which in the case of the CCPA has already passed.

Dedicated privacy units signal aggressive enforcement

All the comprehensive state privacy laws grant their respective state AGs enforcement authority and set a maximum monetary penalty per violation. Notably, the California, Texas, Virginia, and New Hampshire AGs have established a dedicated privacy unit empowered to solely focus on enforcing these laws. This is a red flag to companies operating in those states.

In California, CCPA enforcement began on July 1, 2020, during the pandemic. In November of 2020, California voters approved the California Privacy Rights Act of 2020 (CPRA). The CPRA added new privacy protections to the CCPA, and established a new agency, the California Privacy Protection Agency (CPPA) to implement and enforce the law.

Two years later, California AG Rob Bonta announced the first CCPA settlement with beauty company Sephora, Inc. (Sephora), resolving allegations that the company violated the CCPA.[1]

In the Sephora case, the California AG alleged that Sephora failed to disclose to customers that it sold their data, engaged in the unlawful sale of personal information (including by exchanging data with third parties for analytics information), failed to post a "Do Not Sell My Personal Information" link on its homepage, and failed to respond to or process consumer opt-outs in accordance with "global privacy controls."

After Sephora allegedly failed to cure its violations within a 30-day cure period granted by the California AG, the AG pursued the case against the company and ultimately entered into a settlement that included a $1.2 million penalty, two-year monitoring period, additional reporting requirements, and terms requiring Sephora to review its service provider contracts.

While under newer state laws enforcement actions naturally remain nascent, California AG Rob Bonta has ramped up enforcement under his state's more mature privacy law to pursue violators.

Since Sephora, AG Bonta has secured three additional settlements for alleged violations of the CCPA, including against DoorDash for allegedly failing to notify consumers of the sale of their data, against Glow for failing to properly secure a fertility tracking application, and most recently in June, against Tilting Point Media for allegedly sharing children's data collected from a SpongeBob application without parental consent.

Further, in early 2023, he announced an "investigative sweep" of businesses with mobile applications for allegedly failing to comply with the CCPA. The ongoing sweep targets popular mobile applications in the retail, travel, and food service industries that fail to offer a mechanism for consumers to opt out of data sales or that fail to process consumer opt-out requests, including requests submitted via an authorized agent.

In January of 2024, he announced a sweep of streaming services pursuant to the CCPA. The focus of this most recent investigative sweep is streaming services' compliance with consumers' right to "opt out" of the sale of their personal data under the CCPA. According to AG Bonta, this right should involve minimal steps and should be "easy" for a consumer to accomplish.

AG Bonta initially relied heavily on notice letters granting cure periods for companies to fix potential violations and at one point announced that 75% of the businesses that received a notice-to-cure letter complied within the statutorily prescribed 30 days, with the remaining 25% either still within their 30-day statutory cure period or ultimately coming under active AG investigation for failing to comply.

However, effective January 1, 2023, the automatic, statutory 30-day cure period gave way to discretionary authority granted to the California AG to permit companies to cure on a case-by-case basis.

Therefore, companies that receive a discretionary notice-to-cure letter need to take immediate action and work with legal counsel to develop a strategy to respond and cure violations, if necessary. The breadth of AG Bonta's sweeps serves as notice that no industry or business is immune from regulatory scrutiny.

While California continues to lead the charge in privacy enforcement, Texas appears to be following closely

behind.

In June of this year, Texas AG Ken Paxton announced the launch of a dedicated team housed within his office's Consumer Protection Division focused on "aggressive enforcement of Texas privacy laws," including the Data Privacy and Security Act, the Identify Theft Enforcement and Protection Act, the Data Broker Law, the Biometric Identifier Act, the Deceptive Trade Practices Act (DPTA), and federal laws including the Children's Online Privacy Protection Act (COPPA) and HIPAA.[2]

In his announcement, the AG touted the team as the largest such unit in the U.S. The unit's creation came on the eve of Texas's comprehensive consumer privacy law, the Data Privacy and Security Act, taking effect on July 1. Indeed, AG Bonta has filed actions under these various laws this year as part of this initiative, including privacy actions under the state's "traditional" consumer protection act, the DPTA.

Texas's creation of a specific unit dedicated to privacy enforcement highlights the rapid proliferation of privacy-related laws and underscores a shifting focus toward privacy enforcement in state AG offices.

Many state AGs have previously struggled with marshaling sufficient resources dedicated solely to privacy enforcement, as they are often hamstrung by state budgetary concerns, and have thus assigned such enforcement to existing consumer protection or computer crime divisions. Indeed, the AGs often pool resources to investigate data breaches and privacy-related incidents through multistate coalitions that are part of the National Association of Attorneys General.

Just a couple months after the Texas AG's press release, New Hampshire AG John M. Formella also announced the creation of a new Data Privacy Unit to be housed within the Consumer Protection and Antitrust Bureau of his office. The Unit will be primarily responsible with enforcing compliance with the "New Hampshire Data Privacy Act," which takes effect January 1, 2025.

In the coming months, the unit will be tasked with developing a series of FAQs that will assist consumers and businesses in understanding their rights and responsibilities once the Act becomes effective.[3]The AG is empowered to seek civil penalties of up to $10,000 for each violation, and can also seek criminal penalties of up to $100,000 per violation if there is sufficient evidence that a business is purposely failing to comply with the Act's requirements.

Earlier this year, Virginia AG Jason Miyares also created a privacy enforcement unit within his office's Consumer Protection Section to solely focus on investigating and enforcing Virginia's Consumer Data Protection Act, which took effect on January 1, 2023, and allows for a maximum civil monetary penalty of $7500 per violation.

Avoiding regulatory scrutiny

As privacy law enactments continue, AG privacy enforcement will subsequently increase at an exponential rate across the board, whether through increased funding and resources or office restructuring. Accordingly, companies conducting business with consumers in states with current or pending enforceable privacy laws should verify that they are engaging in defensible privacy and cybersecurity practices in accordance with those states' privacy laws.

Companies must ensure that, at a minimum, they maintain fundamental privacy measures, such as a readily available privacy policy, conspicuous notice of privacy rights, an easily accessible opt-out process on their websites, and consistent fulfillment of consumer opt-out requests. Failure to do so comes with significant risk.

Even in states with pending or no legislation, AGs will likely continue to use existing laws, such as consumer protection acts and data breach notification statutes, to pursue privacy-related enforcement actions, including through multistate investigations and partnerships with other state and federal agencies.

Violations of privacy and consumer protection regulations carry significant financial and reputational risk, and companies should pay close attention to new legislation, guidance, and related enforcement activity from state AGs to ensure preparedness and compliance.

State AGs have historically been at the forefront of regulating emerging technology. Their expertise with enforcing existing laws to shape the regulatory environment, their resources when banded together as a multistate entity, and their agility in responding to novel issues at a local level make them the vanguard regulatory body when it comes to consumer protection in the rapidly evolving technological landscape.

State AGs wield their power by clarifying legislation and regulation through enforcement activity. By leveraging significant real-world experience and detailed industry knowledge, they essentially develop the law to bring about far-reaching changes. Additionally, state AGs employ their growing influence to engage with federal regulators to shape privacy regulation at the national level.

But significantly thus far in 2024, the AGs have sharpened their resources to focus on privacy. Devoting entire units solely to privacy enforcement may signal a sea change within AG offices and a willingness to prioritize privacy over other areas, particularly as cyber incidents and statutory enforcement tools continue to proliferate.

Other AGs will undoubtedly follow suit to demonstrate their own shared commitment to privacy enforcement. Companies handling consumer data must therefore carefully navigate a gauntlet of varying state privacy laws and related enforcement mechanisms, in addition to industry-specific federal regulations.

The increased regulatory scrutiny by California, Texas, Virginia, and New Hampshire highlights the urgency to ensure compliance with state privacy laws. Accordingly, companies must consult skilled legal counsel to ensure they are meeting this rapidly developing patchwork of regulatory standards.

1 California Office of the Attorney General. (2022, August 24). *Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act* [Press Release], https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement.

2 Texas Office of the Attorney General. (2024, June 4). *Attorney General Ken Paxton Launches Data Privacy and Security Initiative to Protect Texans' Sensitive Data from Illegal Exploitation by Tech, AI, and Other Companies* [Press Release], https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-data-privacy-and-security-initiative-protect-texans-sensitive.

3 New Hampshire Office of the Attorney General. (2024, August 15). *Attorney General Formella Announces Creation of New Data Privacy Unit* [Press Release], https://www.doj.nh.gov/news-and-media/attorney-general-formella-announces-creation-new-data-privacy-unit.

RELATED INDUSTRIES + PRACTICES

- Incidents + Investigations
- State Attorneys General