BRACEWELL

Privacy Developments to Watch in 2025

Article

February 04, 2025 | *The Texas Lawbook* | 4 minute read

2024 continued the inexorable march toward state-level comprehensive privacy laws and the conspicuous lack at the federal level. Yet, an assumption that this treatment of comprehensive privacy legislation meant business as usual belies a change that saw privacy as a new battleground.

A Path to Enforcement

Conventional wisdom has it that a private right of action puts enforcement in the hands of the consumer and ensures application of any legislation. The private right of action has long been a sticking point in the federal version of a comprehensive data privacy law, and to date only California has a version of a private right of action.

However, Texas has provided a model for enforcement that could be emulated. The Texas Data Security and Privacy Act leaves enforcement for the law in the hands of the attorney general. The TDPSA provides the mechanism that the attorney general will follow in investigating any claims and, as described below, the penalties that can be recovered.

However, unlike the laws of California, the TDPSA does not expressly call for the creation of a consumer privacy agency, so the Texas attorney general created a Data Privacy and Security Initiative within the Consumer Protection Division of the Office of Attorney General. In essence, the Texas attorney general created, funded and staffed a privacy agency for the enforcement of state and federal privacy laws and the protection of consumer privacy.

And have they ever. Since its creation in June of 2024 — and not including the settlement with Meta Platforms Inc., based on work that preceded the creation of the Privacy Initiative — the Privacy Initiative has announced investigations or

Related People

Lucy
Counsel
HOUSTON
+1.713.221.3328
lucy.porter@bracewell.com

Related Industries

Technology

Related Practices

Data Security & Privacy

lawsuits under the Texas Deceptive Trade Practices-Consumer Protection Act, Texas's Securing Children Online through Parental Empowerment Act and the Texas Data Broker Law.

While the investigation and subsequent settlement with Meta straddled the creation of the Privacy Initiative, the settlement amount, $1.4 billion, explains why this form of enforcement could be a model for other states to follow. The scale of penalties, due to the number of users in any digital space, justifies the investigation. (Penalties under the TDPSA are not to exceed $7,500 per violation and can include recovery of attorney's fees and reasonable expenses. Other laws include penalties from $10,000 per violation to $25,000 per violation.) And the rapidly changing nature of regulations, which provide limited guidance and leave many companies having to choose between overly restrictive interpretations or a more business-friendly approach, means there is usually scope for investigation.

Whether Texas will provide the path for enforcement or be an outlier in privacy activism is yet to be determined, but the activity is worth paying attention to.

Old Laws, New Uses

Not for the first time, 2024 saw old laws brought to the forefront due to their use in regulating the digital space. In Texas, the Meta settlement stemmed from Meta's alleged violations of the state's Capture or Use of Biometric Identifier Act, which has been in effect since 2009. CUBI went largely unenforced until 2022 when the Texas attorney general's office brought suit against Meta for use of its facial recognition software and tagging suggestion program. The rise of the surveillance society coupled with increased use of AI is likely to result in increased use of CUBI and other biometric laws, such as the Illinois Biometric Information Privacy Act.

Staying in Texas for a moment, the Privacy Initiative is also using the DTPA, either alone or in parallel with other privacy laws, as the basis for several of its current investigations. Violations of each of the Data Broker Act, SCOPE Act and Identity Theft Act are violations of the DTPA, which may explain bringing claims under the DTPA. But in at least one instance, the Texas attorney general has opened an investigation based on violations of the DTPA alone.

The use of the DTPA to bring an investigation in the privacy space underscores the importance of being guided by the privacy principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. Arguably, at any time over the last decade DTPA violations could be found that impinged consumer privacy, so the shift now signifies a recognition of harm and an appetite to pursue these types of claims. Every state has a deceptive trade practices

regime, so even states that lack comprehensive privacy legislation could enforce aspects of privacy within that framework.

Beyond Texas, California courts have similarly read new meaning into old laws, expanding the meaning of the California Invasion of Privacy Act to cover cookies and other data collection technologies. Specifically, in a 2023 landmark ruling, *Greenley v. Kochava, Inc.*, a court rejected a motion to dismiss, finding that defendant collected location data via its third-party installed software developer kits without consent of the website visitor and that such activities fall within the definition of the activities that were meant to be constrained under CIPA. Since the *Greenley* decision, a number of cases have been filed in both California state and federal court alleging third-party website tools, such as cookies, web beacons, pixel tags and other similar technologies violate CIPA. Many of these cases have survived demurrer or motion to dismiss, and it is likely a greater number settle without a complaint being filed.

Adding to the possibility of more claims, a recent case attempts to resolve any tension between the California Consumer Privacy Act and the CIPA. In *Mirmalek v. Los Angeles Times Communications LLC*, defendants argued in their motion to dismiss that the requirements of the CCPA should satisfy the notice and consent concerns under CIPA. However, the court in *Mirmalek* found this unpersuasive citing the CCPA itself that "in the event of a conflict between other laws and the provisions of [the CCPA], the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control." The court in *Mirmalek* ensures that the complaints will continue.

Violations of CIPA carry penalties not to exceed $2,500 per violation. Critically, what has enabled the current spate of litigation include the Act's private right of action. Many companies are taking steps to address the gaps, but until clear guidance is offered in the form of legislative action or case law, such complaints are expected to continue.

Conclusion

Advocates of consumer privacy hope this new era of enforcement will result in a greater commitment to data protections. Critics view this as increasing the amount of regulation without offering clarity on compliance. Regardless of your view, the time to start paying attention is now.

Article originally published by The Texas Lawbook on February 4, 2025.