Articles + Publications | September 27, 2024

Takeaways From Texas AG's Novel AI Health Settlement

WRITTEN BY

Sadia Mirza | Stephen C. Piepgrass | Samuel E. "Gene" Fishel | Christopher Carlson

Published in Law360 on September 27, 2024.

On Sept. 18, Texas Attorney General Ken Paxton announced a settlement with healthcare technology company Pieces Technology pursuant to the Texas Deceptive Trade Practices-Consumer Protection Act.

The enforcement action, which sparked backlash from Pieces Technology, represents the first such attorney general settlement pursuant to a state consumer protection act involving generative artificial intelligence. It marks another step in rapidly proliferating state attorney general AI and privacy enforcement. Businesses should thus take notice and plan accordingly to mitigate future regulatory scrutiny.

Settlement Terms

Pieces Technology utilizes AI to assist hospitals and in-patient medical facilities by summarizing, charting and drafting clinical notes for physicians and medical staff.

To measure the accuracy of their AI output related to these services, Pieces developed several metrics and benchmarks. The company advertised the accuracy of its AI product on its website, claiming that it had a critical hallucination rate and severe hallucination rate of less than .001% and less than 1 per 100,000.

AI hallucinations are instances where the output is false or misleading, and Pieces' metrics represent an extremely low incidence of such hallucinations. According to the attorney general's claims, these representations may have violated the DPTA because they were "false, misleading, or deceptive." Under the terms of the settlement, however, Pieces denies any violation of the DPTA.

The settlement is in the form of an assurance of voluntary compliance and requires that moving forward, should Pieces advertise the accuracy of AI products using metrics, it must disclose "the meaning or definition of such metric, benchmark, or similar measurement," and "the method, procedure, or any other process used by Pieces to calculate the metric, benchmark, or similar measurement used in Respondent's marketing or advertising of its products and service."

Further, Pieces is prohibited from making false or misleading statements concerning AI products, and must clearly and conspicuously disclose to all current and future customers any harmful or potentially harmful uses or misuses

of its products.

Notably, the attorney general did not impose a monetary penalty. However, Pieces is required to comply with any future demand from the state to demonstrate its compliance with the settlement for an indefinite period.

The Rise of State Attorney General AI and Privacy Enforcement

State attorneys general are increasingly focusing on regulation of AI as the technology proliferates.

While there are few state laws currently that address AI, state attorneys general have indicated that they will utilize privacy and consumer protection laws to regulate it. In addition to the instant Texas settlement addressing misrepresentation of AI capabilities, the attorneys general have focused on how AI systems utilize personal identifying information, facilitate fraud using deepfakes, and perpetrate bias and discrimination in decision-making processes.

In January, a bipartisan group of attorneys general sent a letter to the Federal Communications Commission, warning of potential fraud where AI is used to imitate human voices in telemarketing campaigns.

In April, Massachusetts Attorney General Andrea Joy Campell issued an advisory detailing how companies can potentially violate the Massachusetts Consumer Protection Act by misrepresenting the reliability of an AI system or falsely advertising the quality of AI systems. The advisory also warns that antidiscrimination laws may be implicated if AI makes decisions based on legally protected characteristics.

In May, Colorado became the first state to enact a law regulating AI use by requiring AI developers to use reasonable care to protect consumers from any known or foreseeable risks of algorithmic discrimination. The Colorado attorney general will have exclusive enforcement authority, with the ability to seek up to $20,000 in civil penalties when the law takes effect on Feb. 1, 2026.

The focus of the state attorneys general aligns closely with a recent shift among attorneys general to devoting increasing resources to privacy enforcement.

In June, 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, and federal laws including the Children's Online Privacy Protection Act and Health Insurance Portability and Accountability Act.[1]

In his announcement, the attorney general touted the team as the largest such unit in the U.S. The unit's creation came on the eve of Texas' comprehensive consumer privacy law, the Data Privacy and Security Act, taking effect on July 1.

Indeed, Paxton has filed additional actions under these various laws this year as part of this initiative, including privacy actions under the DPTA. Based on the Pieces Technology assurance of voluntary compliance, leaders from this new privacy team within the Consumer Protection Division appear to have played an active role in the

investigation and settlement.

Texas' 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 attorney general offices.

Many state attorneys general 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 attorneys general often pool resources to investigate data breaches and privacy-related incidents through multistate coalitions that are part of the National Association of Attorneys General.

California was an early leader in privacy enforcement with the passage of the California Consumer Privacy Act in 2018 and the California Privacy Rights Act of 2020, which established the California Privacy Protection Agency to implement and enforce the law.

California Attorney General Rob Bonta has been active in enforcing these laws having reached settlement for alleged violations with Sephora SA, DoorDash Inc., Glow Inc. and Tilting Point Media LLC over the past two years, and announcing ongoing investigative sweeps of businesses with mobile applications and streaming services to ensure CCPA compliance.

Given the recent proliferation of AI, it is only natural that California will scrutinize companies' deployment of AI in light of potential violations of the CCPA and CPRA.

New Hampshire Attorney General John 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 for enforcing compliance with the "New Hampshire Data Privacy Act," which takes effect Jan. 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.[2]

And Virginia Attorney General 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 Jan. 1, 2023.

Implications for Businesses

Companies conducting business with consumers in multiple states should verify that they are engaging in defensible privacy and cybersecurity practices in accordance with those states' consumer protection and privacy laws, particularly if using AI.

Regarding AI systems, companies need a firm grasp of the system's foundational model and its capabilities, and should perform a thorough risk assessment before employing AI products.

Companies must also ensure that, at a minimum, they maintain fundamental privacy measures connected with AI use, 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. 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 attorneys general to ensure preparedness and compliance.

Beyond these general privacy considerations, businesses advertising the use of AI products must be alert that they are potentially subject to state consumer protection acts and Federal Trade Commission scrutiny if such advertising contains false or misleading claims. Such scrutiny will only increase in the wake of the Pieces Technology settlement.

Recognizing this risk, the FTC has developed guidance for companies employing AI products and advertising their capabilities.[3] The guidance warns against exaggerating what an AI product can do and notes that claims that lack scientific support or apply to only certain users or certain conditions could be considered deceptive.

Companies must also be aware of reasonably foreseeable risks and impacts that the AI system poses, and that, if something goes wrong, the company cannot simply blame the developer.

Finally, the agency warns against labeling something as “AI powered” when it actually is not, noting “merely using an AI tool in the development process is not the same as a product having AI in it.”

Companies considering implementing AI systems in their businesses must prepare for potential exposure under a patchwork of state consumer protection and privacy laws, and associated federal and state regulatory scrutiny.

To mitigate this risk, all levels of decision-makers, including executives, IT staff and legal counsel, should be aware of the risks and capabilities of AI systems, and should be involved in their implementation.

---

[1] Texas Office of the Attorney General. (2024, June 24). 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.

[2] 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.

[3] Federal Trade Commission (2023, February 27), Keep Your AI Claims in Check. https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check.

RELATED INDUSTRIES + PRACTICES

- Artificial Intelligence

- Privacy + Cyber