SIDLEY

UPDATES

Rising AI Enforcement: Insights From State Attorney General Settlement and U.S. FTC Sweep for Risk Management and Governance

December 10, 2024

On September 18, 2024, Texas announced a first-of-its-kind state AG **settlement** against generative artificial intelligence (AI) healthcare company Pieces Technologies (Pieces) for using allegedly deceptive and misleading statements regarding the accuracy and safety of its products. On September 25, 2024, the U.S. Federal Trade Commission (FTC) announced an enforcement sweep, called Operation AI Comply, alleging that certain companies used AI technology in violation of the FTC Act's prohibition on deceptive and unfair practices. More recently, on December 3, 2024, the FTC issued an order against AI-powered facial recognition technology provider IntelliVision Technologies Corp. that provides important insight into how the commission will review claims of AI bias and efficacy. These developments are described in more detail below, along with key takeaways for businesses.

Texas AG Settlement With Pieces

The Pieces settlement resulted from an enforcement action alleging that Pieces "deployed its products at Texas hospitals after making a series of false and misleading statements about the accuracy and safety of its [generative AI] products" that synthesize and summarize patient charts and notes. The case was brought under the Texas Deceptive Trade Practices Consumer Protection Act (DTPA) — alleging that Pieces' representations may have violated the DTPA due to their false, misleading, or deceptive nature. Specifically, the Texas AG alleged that Pieces developed metrics supporting its claim that its healthcare AI products were "highly accurate" (including claims that its products have a "critical" and "severe hallucination rate" of "<.001%" and "<1 per 100,000") but that these metrics were allegedly inaccurate and deceived hospitals about the safety and accuracy of Pieces products.

As part of the settlement, Pieces did not pay a monetary settlement but agreed to the following key assurances:

- **Clear and Conspicuous Disclosures — Marketing and Advertising.**Pieces agreed to clearly and conspicuously disclose the definition of any metrics used to describe the output of its generative AI products as well as the methods used to calculate such metrics.
- **Prohibitions Against Misrepresentations.** Pieces cannot make any false, misleading, or

unsubstantiated representations regarding any feature, characteristic, function, testing, or appropriate use of any of its products. Pieces also may not misrepresent or mislead any customer or user regarding the accuracy, functionality, purpose, or any other feature of its products.

- **Clear and Conspicuous Disclosures — Customers.** Pieces must also provide all current and future customers with documentation that clearly and conspicuously discloses any known or reasonably known harmful or potentially harmful uses or misuses of its products or services. The settlement does not go so far as to specify how exactly the company identify or test for known or reasonably known or potentially harmful uses or misuses. However, it does indicate that documentation for customers should include at minimum
    - the types of data and/or models used to train the AI technologies
    - detailed explanation of the intended purpose and use of the technology
    - any training or documentation needed to ensure proper use of the products and services
    - any “known or reasonably knowable, misuses of a product or service that can increase the risk of inaccurate outpoints or increase the risk of harm to individuals”
    - documentation reasonably necessary for a user of the AI technologies to understand the nature and purpose of the AI output, how to monitor for patterns of inaccuracy, and how to “reasonably avoid” misuse of the products and services

This settlement reflects recent policy shifts toward aggressive privacy and consumer protection enforcement by the Texas AG. In June 2024, the Office of the Attorney General **announced** the creation of an initiative to enhance enforcement of the DTPA and the state’s privacy, biometric, identity theft, and data broker laws.

FTC’s Operation AI Comply

On September 25, 2024, the FTC **announced** cases against five companies that allegedly used AI in unfair or deceptive ways in violation of federal consumer protection laws. The five Operation AI Comply cases target both the use of AI-powered tools that can allegedly magnify deceptive or unfair business activities as well as overstatements and AI “hype” to attract consumers:

- **DoNotPay.** In an administrative complaint, the FTC alleges that DoNotPay made misleading statements about the capabilities of its “AI lawyer” subscription service. A proposed settlement would require DoNotPay to pay $193,000, inform certain subscribers about the FTC’s case, and cease its allegedly misleading practices.
- **Ascend Ecom.** The FTC alleges in a complaint filed in California federal court that Ascend Ecom and its affiliates made deceptive claims about earnings to entice customers to invest in “risk free” AI business opportunities. Then, the FTC further alleges, Ascend refused to pay customers back when the investments did not yield returns and threatened customers who attempted to publish reviews about the scheme.
- **Ecommerce Empire Builders.** The FTC filed a complaint in Pennsylvania federal court alleging

that Ecommerce Empire Builders made deceptive claims about AI-driven investment tools, improperly promising thousands of dollars in returns per month. The company also allegedly failed to make certain disclosures about the investment tools and required customers to agree not to post negative reviews about their services.

- **FBA Machine.** In a complaint filed in New Jersey federal court, the FTC alleges that FBA Machine made deceptive and misleading statements about possible returns from online storefronts powered by AI software, resulting in nearly $16 million in consumer losses. The FTC obtained an order temporarily halting FBA Machine's business practices.
- **Rytr, LLC.** According to the FTC's administrative complaint, customers of Rytr, LLC could use the company's subscription-based AI writing assistant to generate false reviews for their products or services, which Rytr's customers then used to deceive their own customers. Rytr and the FTC have reached a proposed settlement that would prohibit Rytr from continuing to offer any service that generates user reviews.

IntelliVision Technologies. The FTC took a step further to wade into how companies should substantiate AI claims with its most recent AI settlement of the FTC's investigation into IntelliVision Technologies's representations that its AI-powered facial recognition software is "without racial bias" or has "zero gender or racial bias." The FTC found that IntelliVision deceived its customers when it proclaimed its facial recognition software has "zero gender or racial bias." The FTC found that IntelliVision's software was similar to other facial recognition software in that "[t]he accuracy rates … vary depending on the demographics, including the race and gender of image subjects." In particular, such software often produces "more false positive 'matches' for certain demographics, including West and East African, East Asian and American Indian than for images of Eastern European faces" and also produces more false positives in women than in men. The FTC alleged that IntelliVision was no exception: "[E]rror rates for IntelliVision's algorithms differed across different demographics, including region of birth and sex." Accordingly, the FTC took the position that IntelliVision could not advertise its product as having "zero gender or racial bias."

Commissioner Andrew Ferguson elaborated on the definition of "bias" in a concurring statement. Rejecting a definition of bias as requiring "equal false-negative and false-positive rates across race and sex groups," Commissioner Ferguson nonetheless warned that "[i]f [IntelliVision] intended to invoke a specific definition of 'bias,' it needed to say so. But it did not say so; it instead left the resolution of this ambiguity up to consumers. IntelliVision must therefore bear the burden of substantiating all reasonable interpretations that consumers may have given its claim that its software had 'zero gender or racial bias.' "

Significantly, the settlement orders IntelliVision to make no further claims with respect to the efficacy or bias of its AI (or its ability to withstand spoofing) unless those claims are based on "competent and reliable testing" at the time the claim is made, which is documented in detail. Critically, to substantiate a claim, the FTC considers competent and reliable testing under the order to be "testing that is based on the expertise of professionals in the relevant area, and that (1) has been conducted and evaluated in an objective manner by qualified persons and (2) is generally accepted by experts in the profession to yield accurate and reliable results…."

The enforcement landscape. Critically, regulators are leveraging preexisting authority under the FTC

Act to address the various uses — and potential misuses — of AI technology. In addition to the unfa and deceptive practices theory of liability underpinning the Texas AG and FTC activity, there are other sources of legal risk for companies that develop or use AI. Several state privacy laws, including Texas', require companies to conduct a risk assessment before using AI technology to profile consumers in furtherance of decisions related to the provision or denial of financial services, housing, healthcare, or employment opportunities. These laws also allow consumers to opt out of the use of their personal data for certain kinds of profiling decisions. Other federal agencies are also considering use of their existing regulatory authorities to regulate and enforce in an AI context. Indeed, earlier this year the Department of Justice (DOJ) **signaled** its intent to not only use existing enforcement authority to tackle new challenges posed by AI technology but also to seek enhanced penalties where actors use AI to perpetrate wrongdoing. The DOJ also recently updated guidelines for prosecutors to evaluate the effectiveness of corporate compliance programs to manage AI risk. This **guidance** emphasizes the company's processes to identify and manage emerging risks, including the extent a company monitors and tests its AI to evaluate whether the AI is functioning as intended and in compliance with the company's policies and how quickly the company can identify and remediate decisions made by AI that contradicts policies or company values.

All this enforcement activity makes clear that although the U.S. may not yet have comprehensive federal AI regulation (and Colorado's comprehensive AI law — the first of its kind in the U.S. — does not take effect until 2026), regulators are already using existing legal tools to address perceived harms and risks of AI.

Key Takeaways for Businesses Developing or Using AI Products and Services

- Regulators are not waiting for federal AI regulation or AI-specific state laws to enforce in this space; AI issues are being enforced on a wide range of existing laws, including consumer protection and privacy laws.
- Marketing claims related to AI technologies in products will be scrutinized for inaccuracies, overstatements, or other deception concerns. Heightened disclosures and transparency around the basis for marketing claims, risks of AI technologies, and how to properly use the technologies for their intended uses in a way to reasonably mitigate risks are important for commercialization. This is particularly crucial for companies offering AI products or services for higher-risk applications that may affect individual consumers, such as healthcare, financial services, and education.
- Business-to-business (B2B) companies are not immune from enforcement actions in this space. Regulators are targeting all companies, regardless of whether they are consumer-facing companies or B2B companies interacting with sophisticated counterparties.

For more on what businesses should keep in mind when assessing AI legal risks, we encourage you to consider this **additional resource**, visit the **Sidley AI Monitor**, or contact one of the Sidley lawyers listed below.

CONTACTS

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work, or

Colleen Theresa Brown, Partner	+1 202 736 8465, ctbrown@sidley.com
Benjamin M. Mundel, Partner	+1 202 736 8157, bmundel@sidley.com
Lauren C. Freeman, Counsel	+1 415 772 1253, lfreeman@sidley.com
Garrett M. Lance, Managing Associate	+1 214 969 3513, glance@sidley.com
Christina C. Koenig, Managing Associate	+1 214 969 3583, christina.koenig@sidley.com

Attorney Advertising—Sidley Austin LLP is a global law firm. Our addresses and contact information can be found at www.sidley.com/en/locations/offices.

Sidley provides this information as a service to clients and other friends for educational purposes only. It should not be construed or relied on as legal advice or to create a lawyer-client relationship. Readers should not act upon this information without seeking advice from professional advisers. Sidley and Sidley Austin refer to Sidley Austin LLP and affiliated partnerships as explained at www.sidley.com/disclaimer.

© Sidley Austin LLP