

AI IS NOW THE DOMAIN OF STATE AGS AND BUSINESSES SHOULD TAKE NOTICE

By Gene Fishel and Nick Gouverneur

While artificial intelligence (AI) in some form has existed for decades, *generative* AI, the ability of AI systems to create new content, has only recently exploded into the public domain and become a powerful force in the global economy. Generative AI provides myriad opportunities for businesses to improve products, processes, and analytics in an efficient and cost-effective manner. Naturally, a large contingent of companies has embraced this helpful technology; however, those that do must be aware of attendant pitfalls, including regulatory exposure.

States typically serve as regulatory laboratories, and state regulators, including most notably state attorneys general (AGs), are increasingly turning their attention to potential dangers as AI proliferates. Although there are currently few state laws specifically addressing AI, AGs have signaled that existing privacy and consumer protection laws can cover AI use. Specifically, AG enforcement priorities include how AI systems handle personal identifying information, the role of AI in facilitating fraud, and the potential for bias and discrimination

in AI-driven decision-making processes. Businesses thus need to thoroughly evaluate any AI deployment and stay abreast of AG action and emerging legislation to mitigate regulatory and litigative risk.

THE AGS ACT IN 2024

State AGs increasingly sounded alarms about potential AI harms during 2024. In January, Pennsylvania AG Michelle Henry sent a comment letter to the Federal Communications Commission (FCC), warning about the dangers associated with AI when used by telemarketers and requesting that the FCC strongly restrict such usage.¹ Specifically, Henry noted that “marketers wanting to use A.I. to impersonate a human voice should be required to follow the TCPA’s [Telephone Consumer Protection Act] rules and regulations with respect to artificial voices, including obtaining the prior express written consent from consumer targets.”² Democratic AGs from 26 other states joined the letter.

Continued on page 13

Gene Fishel is a member of the Troutman Pepper Hamilton Sanders LLPs Regulatory Investigations, Strategy + Enforcement (RISE) practice, based in the Richmond office. Gene formerly served as Senior Assistant Attorney General and Chief of the Computer Crime Section in the Office of the Attorney General of Virginia and as Special Assistant United States Attorney in the Eastern District of Virginia for 20 years. **Nick Gouverneur** is an associate in Troutman Pepper’s Regulatory Investigations, Strategy + Enforcement Practice Group.

AI IS NOW THE DOMAIN OF STATE AGS AND BUSINESSES SHOULD TAKE NOTICE	1
IN BRIEF	3



Wolters Kluwer

AI is Now the Domain of State AGs from page 1

Minnesota AG Keith Ellison has dedicated resources to understanding how AI and social media affect young people. In February, Ellison released a report detailing an investigation into how “the integration of increasingly powerful AI into more algorithms is likely to accelerate” the trend of excessive technology use at the expense of more productive activities, such as “sleep and in-person socialization.”³ The report makes recommendations to combat these troubling trends, primarily focusing on regulating the behavior of those that disseminate content over social media rather than social media consumers. The recommendations include banning design features geared at maximizing platform usage, providing aggressive privacy defaults to limit unwanted content sharing, mandating rate limits to hamper the ability of small groups of users to conduct manipulation campaigns, and more.⁴

Also in February, Republican AG Sean Reyes of Utah sent a comment letter responding to the U.S. Department of Commerce’s request for information on the regulation of AI.⁵ The letter focused on President Joe Biden’s Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI. It decried the president’s attempt to “to centralize governmental control over an emerging technology being developed by the private sector... [and] open[ing] the door to using the federal government’s control over AI for political ends.”⁶ This position promotes a decentralized, state-based approach to AI regulation.

Massachusetts AG Andrea Joy Campbell issued an advisory “white paper” in April, explaining how “developers, suppliers, and users of AI systems” could potentially violate the Massachusetts Consumer Protection Act through misrepresentations regarding AI’s reliability or by falsely advertising the quality of AI systems.⁷ The advisory also warned those using AI that “algorithmic decision-making that relies on or uses discriminatory inputs [or] that produces discriminatory results, such as those that have the purpose or effect of disfavoring or disadvantaging a person or group of people based on a legally protected characteristic” violate Massachusetts’s anti-discrimination law.⁸

Just before the election, New York AG Letitia James released a consumer alert to remind voters that AI chatbots will not provide accurate information about where, when, or how to vote.⁹ Her office tested different chatbots and found that each had the tendency to return inaccurate information.

Moreover, the continued proliferation of state comprehensive privacy laws and the AG’s increased focus overall on privacy-related enforcement in 2024 will also have an impact on AI development and deployment. 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 sought to enact their own privacy legislation. In 2023, seven states passed comprehensive consumer privacy laws, and six more were enacted in 2024, bringing the total to 19 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.

In January 2024, California AG Rob Bonta launched an “investigative sweep” of streaming services pursuant to the CCPA.¹⁰ The initiative targeted streaming services’ compliance with consumers’ right to “opt out” of the sale of their personal data. Bonta emphasized that this process should be straightforward and require minimal effort from consumers. This followed a 2023 sweep of businesses with mobile applications that allegedly failed to comply with the CCPA. That sweep targeted popular mobile applications in the retail, travel, and food service industries that failed to offer a mechanism for consumers to opt out of data sales or that failed to process consumer opt-out requests, including requests submitted via an authorized agent.

In June, Texas AG Ken Paxton announced the formation of a dedicated team within his Consumer Protection Division to prosecute and enforce Texas’ privacy laws, including the state’s new comprehensive consumer privacy law, the Data Privacy and Security Act.¹¹ This unit, touted as the largest of its kind in the U.S., will aggressively enforce privacy laws, including the Identify Theft Enforcement and Protection Act, the Data Broker Law, the Biometric Identifier Act, the Deceptive Trade Practices Act, and federal laws such as the Children’s Online Privacy Protection Act (COPPA) and HIPAA.¹²

Soon after this announcement, Paxton announced a settlement pursuant to the Texas Deceptive Trade Practices – Consumer Protection Act (DPTA), representing the first such AG settlement pursuant to a state consumer protection act involving generative AI.¹³ Texas accused a health care technology company of advertising misleading AI accuracy metrics. The company agreed to settle via an assurance of voluntary compliance without admitting any violation. The settlement mandates that the company clearly define and disclose the methods used to calculate any advertised metrics, avoid false or misleading statements,

and inform customers of any potentially harmful uses of its AI products for an indefinite period.¹⁴

In August, New Hampshire AG John H. Formella formed a Data Privacy Unit within the Consumer Protection and Antitrust Bureau of his office. The unit is tasked with enforcing compliance with the New Hampshire Data Privacy Act, which takes effect on January 1, 2025. Currently, the unit is developing a set of FAQs to assist consumers and businesses in understanding their rights and responsibilities once the act takes effect.¹⁵

EMERGING AI LEGISLATION AND REGULATION

Several states have either enacted laws or introduced legislation and regulations over the past year to address AI developments and the attendant risks they pose to businesses and consumers.

In May, Colorado became the first state to enact a law requiring developers of AI systems to use “reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination in the high-risk system.”¹⁶ Compliance with certain provisions, such as “[d]isclosing to the attorney general and known deployers or other developers of the high-risk system any known or reasonably foreseeable risks of algorithmic discrimination,” creates a rebuttable presumption that a developer used reasonable care.¹⁷ The Colorado AG is authorized to enforce the statute and can seek up to \$20,000 in civil penalties once the law takes effect on February 1, 2026.

In September, California Governor Gavin Newsom signed more than a dozen AI-focused bills into law, addressing concerns from AI transparency and risk management, to privacy and the ethical use of AI in health care and education, with many of the bills enforceable by the California AG.¹⁸ Among the significant new laws, AB-1008 expands California’s privacy framework to include generative AI systems, ensuring that personal data exposed by AI is subject to strict privacy protections.¹⁹ SB-942 requires AI-generated content to be clearly marked, helping the public identify such content.²⁰ Additionally, AB-2885 establishes a formal legal definition of AI, providing a clearer regulatory framework.²¹ In education, AB-2876 and SB-1288 promote AI literacy and the exploration of AI’s role in public education, preparing students for a future where AI is increasingly prevalent.²²

AB-2013 mandates transparency in AI training data, requiring companies to disclose detailed

information about their datasets.²³ SB-896 focuses on AI risk management, directing California’s Office of Emergency Services to collaborate with leading AI companies to assess potential threats to state infrastructure.²⁴ Additionally, new regulations like AB-3030 and SB-1120 aim to ensure the responsible use of AI in health care, requiring disclosures and oversight by licensed physicians.²⁵ These examples reflect a comprehensive approach to AI regulation, addressing both the opportunities and risks associated with the technology.

In October, Texas Representative Giovanni Capriglione released a draft bill to regulate AI that he plans to introduce in 2025 legislative session.²⁶ The “Texas Responsible AI Governance Act” creates a comprehensive AI governance framework aimed at addressing ethical deployment and safeguarding fundamental rights. The 41-page draft, developed with input from more than 300 industry experts, focuses on preventing algorithmic discrimination in automated decision-making systems.²⁷ The bill exempts research and testing AI models under a “sandbox program” and does not cover low-risk AI systems.

The proposed Texas legislation requires developers and deployers of high-risk AI systems to take measures to prevent discrimination, including regular testing and compliance checks. The bill also mandates consumer notification when interacting with high-risk AI systems and provides the right to appeal AI-driven decisions. It prohibits the use of AI for manipulating behavior, social scoring, and collecting biometric data, with enforcement by the state’s AG and fines up to \$100,000 for violations. The bill also includes provisions for an AI workforce development grant program to prepare Texas workers and students for the AI industry.²⁸

IMPLICATIONS FOR BUSINESSES

State AGs have historically been at the forefront of regulating emerging technology. Their expertise 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, AGs employ their growing

influence to engage with federal regulators to shape privacy regulation at the national level.

In 2024, the AGs sharpened their resources to focus on AI and privacy. Devoting entire units solely to privacy enforcement may signal a sea change within AG offices and a willingness to prioritize privacy (and consequently AI use) 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 AI and privacy laws and related enforcement mechanisms, in addition to industry-specific federal regulations. The increased regulatory scrutiny by California, Colorado, Massachusetts, New Hampshire, and Texas highlights the urgency to ensure compliance with these laws. Accordingly, companies must consult skilled legal counsel to ensure they are meeting this rapidly developing patchwork of regulatory standards.

As AI and privacy law enactments continue, related AG enforcement will naturally increase at an exponential rate across the board, whether through increased funding and resources or office restructuring. Companies conducting business with consumers and using AI in states with current or pending enforceable AI and privacy laws should verify that they are engaging in defensible privacy and cybersecurity practices in accordance with those states' laws. Companies must ensure that, at a minimum, they maintain fundamental privacy measures, such as a readily available privacy policy that includes how they utilize AI, 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, anti-discrimination laws, data breach notification statutes, and general consumer privacy laws, to pursue AI-related enforcement actions, including through multistate investigations and partnerships with other state and federal agencies. Violations of these laws 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.

NOTES

1. Pa. Off. of Att'y Gen., Reply Comment of 26 State Attorneys General (Jan. 2024), <https://www.attorneygeneral.gov/wp-content/uploads/2024/01/2024-01-16-Reply-Comment-of-State-AGs-FCC-AI-NOI.pdf>.
2. *Id.*
3. OFF. OF MN. ATT'Y GEN. KEITH ELLISON, MINNESOTA ATTORNEY GENERAL'S REPORT ON EMERGING TECHNOLOGY AND ITS EFFECTS ON YOUTH WELL-BEING, at 5–6 (2024), <https://www.ag.state.mn.us/Office/Reports/EmergingTechnology.pdf>.
4. *Id.* at 22.
5. Utah Off. of Att'y Gen., Re: Comment by States of Utah, Alabama, Arkansas, Florida, Idaho, Iowa, Kansas, Louisiana, Mississippi, Missouri, Montana, Nebraska, North Dakota, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, Virginia, and West Virginia on RFI Related to NIST's Assignments under Sections 4.1, 4.5 and 11 of the Executive Order Concerning Artificial Intelligence (Feb. 2, 2024), https://attorneygeneral.utah.gov/wp-content/uploads/2024/02/2024-02-02_Comment_response_letter_on_NIST_RFI_re_AI.pdf.
6. *Id.* at 2.
7. Mass. Off. of Att'y Gen., Attorney General Advisory on the Application of the Commonwealth's Consumer Protection, Civil Rights, and Data Privacy Laws to Artificial Intelligence (Apr. 16, 2024), <https://www.mass.gov/doc/ago-ai-advisory-41624/download>.
8. *Id.*
9. Off. of the N.Y. State Att'y Gen., Consumer Alert: Attorney General James Warns Voters Against Relying on AI Chatbots for Election Questions (Nov. 1, 2024), <https://ag.ny.gov/press-release/2024/attorney-general-james-warns-voters-against-relying-ai-chatbots-election>.
10. Attorney General Bonta Announces Investigative Sweep, Focuses on Streaming Services' Compliance with the California Consumer Privacy Act, Cal. Off. of the Att'y Gen. (Jan. 26, 2024), <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-investigative-sweep-focuses-streaming-services%E2%80%99>.
11. Tex. Off. of Att'y Gen., Attorney General Ken Paxton Launches Data Privacy and Security Initiative to Protect Texans' Sensitive Data from Illegal Exploitation by Tech, AI, and Other Companies (June 4, 2024), <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-data-privacy-and-security-initiative-protect-texans-sensitive>.
12. *Id.*
13. Tex. Off. of Att'y Gen., Attorney General Ken Paxton Reaches Settlement in First-of-its-Kind Healthcare Generative AI Investigation (Sept. 18, 2024), <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-reaches-settlement-first-its-kind-healthcare-generative-ai-investigation>.
14. *Id.*
15. *Id.*
16. S.B. 24-205, 74th Gen. Assemb., Reg. Sess. (Col. 2024), <https://leg.colorado.gov/bills/sb24-205>.
17. *Id.*
18. Press Release, Governor Gavin Newsom, Governor Newsom announces new initiatives to advance safe and responsible AI, protect Californians (Sept. 29, 2024) (<https://www.gov.ca.gov/2024/09/29/governor-newsom-announces-new-initiatives-to-advance-safe-and-responsible-ai-protect-californians>).
19. *Id.*
20. *Id.*
21. *Id.*
22. *Id.*
23. *Id.*
24. *Id.*
25. *Id.*
26. See Texas Responsible AI Governance Act (TRAIGA), <https://www.documentcloud.org/documents/25257148-texas-responsible-ai-governance-act-traiga-1>.
27. *Id.*
28. *Id.*



Wolters Kluwer
Journal of Internet Law
Distribution Center
7201 McKinney Circle
Frederick, MD 21704

To Subscribe to JOURNAL OF INTERNET LAW, Call 1-800-638-8437