View on our website.

State Attorneys General (AG) Task Force | Artificial Intelligence Update

October 16, 2025

Balancing Support for Federal Frameworks with Enforcement Autonomy: State Attorneys General Approaches to Youth Online Protections and Artificial Intelligence

Gibson Dunn has extensive experience advising multinational companies operating online services on a wide variety of regulatory and law enforcement investigation, enforcement, strategic counseling, litigation, and appellate matters relating to youth online safety, including on privacy and AI-related issues.

The regulatory landscape governing safeguards around children's online protection is evolving rapidly. While State Attorneys General (State AGs) are using existing statutes to increase enforcement efforts, a large number simultaneously support omnibus youth privacy legislation at the federal level. Meanwhile, many State AGs have opposed a federal Artificial Intelligence (AI) framework if such a law comes at the expense of states' autonomy in AI oversight.

A. State AG Enforcement of Youth Issues: Regulation by Action & Policy Discourse

State AGs are not waiting for Congress to pass legislation relating to youth[1] online activity. Although State AGs have continuously advocated at the federal level for policy change, they have recently turned a focus towards enforcing existing privacy, consumer protection, child

safety, and unfair competition laws. Social media platforms have been targets for such actions in the past, but there also is an increasing focus towards services not solely associated with children—like streaming services—with State AGs now probing companies on issues such as data monetization of minors. Many of these actions leverage general-purpose statutes, revealing a trend of regulation by enforcement in the absence of updated legislation.

1. State AG Investigation and Litigation

State AGs have frequently initiated action under state consumer protection frameworks to address a full range of youth protection issues, including those implicating privacy and artificial intelligence (AI) concerns. While some State AGs are more active than others (New York and Texas have shown a particular interest in this area), this a broad trend across states.

For example, in August, 44 State AGs issued a letter to 13 technology companies, asserting that failure to protect children will result in enforcement actions from the states. The letter raised concerns about the potential for AI chats to expose children to sexualized content. The outreach follows a similar letter in May 2025, issued by a coalition of 28 State AGs, which was prompted by reports of sexually explicit AI. In May, the State AGs sought responses regarding a technology company's safeguards, content moderation practices, and plans to prevent further misuse of its AI technologies.

In addition, recent representative State AG enforcement and regulatory developments include:

Alabama. On April 29, Alabama's Attorney General filed a complaint against a social media company under its deceptive trade practices law and for alleged wantonness and negligence pursuant to allegations that the company exploits children on its platform, among other things. The state is positioning the case as part of a broader effort to hold social media platforms accountable for their alleged impact on children's well-being.

Michigan. On April 30, Michigan's Attorney General filed a complaint against a streaming platform alleging systemic violations of Michigan consumer protection laws and the Children's Online Privacy Protection Act (COPPA). The complaint alleges that the streaming service collects and monetizes personal data from children under the age of 13—including voice recordings, geolocation, IP addresses, and browsing histories—without obtaining verifiable parental consent or providing adequate notice. The AG asserts that the streaming platform lacks child-specific user profiles, thereby exposing minors to the same data collection practices as adults, and further alleges that the service facilitates third-party access to children's data through partnerships with advertisers and data brokers, some of whom have been previously sanctioned by the FTC. Michigan is positioning the case as part of a broader regulatory push to enforce digital privacy standards for minors.

Missouri. In September 2025, the Missouri's Attorney General's office announced an age-verification regulation for websites and platforms where one-third or more of content is pornographic or sexually explicit. The regulation is promulgated under the Missouri Merchandising Practices Act, Missouri's UDAP law which prohibits unfair and deceptive acts or practices. Failure to comply with the age-verification requirements will constitute an "unfair practice" under the Act. Missouri's approach represents a novel one, as states have otherwise

used statutes to impose age-verification requirements. The regulation will go into effect on November 30, 2025.

New Hampshire. In June 2024, the New Hampshire attorney general sued a social media company alleging that the platform's design and operations harm the mental health of young users in violation of the state's Consumer Protection Act (New Hampshire's UDAP law which prohibits unfair and deceptive acts or practices). The Complaint also includes tort theories under strict liability and negligence for the allegedly "addictive features" of the platform. On July 8, 2025, the New Hampshire state Superior Court denied in large part a social media company's motion to dismiss New Hampshire's claims. The ruling found the State has standing to pursue consumer protection and public health claims on behalf of its residents, particularly minors, and signals judicial receptiveness to state-led efforts to regulate social media platforms through existing consumer protection frameworks. This decision may embolden other jurisdictions pursuing similar litigation and underscores the growing legal scrutiny of these platforms.

New Jersey. On April 17, New Jersey's Attorney General filed a civil complaint in New Jersey state court against a communication platform alleging that the company violated the New Jersey Consumer Fraud Act and other state laws by failing to implement adequate safeguards to protect minors from harmful and illegal content on its platform. The complaint asserts that the platform knowingly facilitates access to graphic content—including sexual exploitation, self-harm, and drug-related material—though it markets itself as a safe space for youth. The State alleges that the company's design choices and content moderation practices contribute to a public health crisis among youth and mislead consumers about the platform's safety. New Jersey is positioning the case as part of a broader multistate initiative to hold tech companies accountable for the mental health impacts of their platforms on youth.

New York. In September 2025, New York Attorney General James issued proposed rules for compliance with New York's Stop Addictive Feeds Exploitation (SAFE) for Kids Act.[2] The proposed rules identify "addictive feed" as an online platform, or portion of one, where media is "shared or generated by users" and "concurrently or sequentially, recommended, selected, or prioritized for display" based on either (i) "information persistently associated with the user or the user's device" or (ii) the user's previous online behavior including interactions with media generated on that platform or a different platform. The proposed rules make it unlawful for any covered operator (defined by the rules to mean a platform where monthly active users spend at least 20% of their time on an "addictive feed") to provide an "addictive feed" to minors without parental consent. Absent parental consent, the rules also prohibit notifications to users between 12 a.m. and 6 a.m. (nighttime notifications) from covered operators.

Texas. In early 2025, Texas initiated broad investigative actions across numerous AI and platform operators, asserting precedent as "the largest data privacy and security initiative of any State AG office." Specifically, the AG launched an investigation into 15 technology companies for potential violations of the state's SCOPE Act[3] (Securing Children Online Through Parental Empowerment), which mandates parental consent for minors' data collection and prohibits the sale of such data without authorization, and has already served as the basis of an action in late 2024 two months after the law's effective date.

2. State AG Reporting: Shaping Tech Policy

Not only are State AGs bringing enforcement actions against tech companies, they are shaping the discourse around existing and emerging technologies accessible to youth. In September 2023, the National Association of Attorneys General (NAAG) sent a letter to Congress regarding *Artificial Intelligence and the Exploitation of Children*, calling on Congress to establish an expert commission "to study the means and methods" of AI "used to exploit children", and to "propose solutions to deter and address such exploitation in an effort to protect America's children." NAAG highlighted protecting children "from the dangers of AI." The following year, NAAG sent a letter to Congress on *Requiring a Surgeon General's Warning Label on Social Media Platforms*, calling on lawmakers to pass legislation requiring a U.S. surgeon general warning on all algorithm-driven social media platforms.

Several State AGs also have released reports relating to emerging technology, including AI, as it relates to youth. For example, in February 2025, the Minnesota AG released a report examining design features purporting to cause harm to young people and providing policy recommendations to the state legislature.

These letters and reports signal State AGs are moving beyond case-by-case enforcement into agenda-setting, using research and public statements to advance their priorities.

B. State AG Support for Youth Privacy Legislation at the Federal Level: COPPA 2.0 and KOSA

State AGs have also expressed support for two federal legislative efforts aimed at youth online privacy and safety: (i) updating the existing framework in the Children's Online Privacy Protection Act (COPPA); and (ii) proposing a new, supplemental youth protections regime under the Kids Online Safety Act (KOSA). Both signal efforts to reduce the patchwork of state-by-state approaches, while giving robust enforcement authority to State AGs.

1. Children's Online Privacy Protection Act

In March 2024, NAAG sent a letter to the FTC on behalf of a bipartisan coalition of 43 State AGs urging the federal government to update and strengthen the COPPA Rule—enforceable by both the FTC and State AGs—which governs how companies collect and process the data of children under the age of 13. The State AGs advocated to broaden the definitions of personal data to include for example, biometric identifiers and avatars generated from a child's image and likeness. On January 16, 2025, the FTC voted 5-0 to approve updates to the COPPA Rule which was last updated over a decade ago, in 2013.[4]

On April 22, 2025, the FTC published the final amendments to the COPPA Rule in the Federal Register. The published amendments became effective on June 23, 2025, and operators will have until April 22, 2026 to come into full compliance (except for FTC-approved COPPA safe harbor programs, which must comply with certain amendments that specify earlier compliance dates). Violations of the updated COPPA Rule carry civil penalties up to $53,088 per violation for 2025.[5]

2. Kids Online Safety Act

In November 2024, a coalition of 32 State AGs penned an open letter to Congress to pass KOSA, which was first introduced in February 2022, and which purports to enhance online safety for minors beyond COPPA. First, KOSA would apply to youth ages 16 and under, as compared to COPPA which is applicable to youth ages 13 and under. Second, KOSA would require social media and other technology providers to take measures to reduce harms to minors, including mental health issues, addiction-like behaviors, sexual exploitation, and exposure to harmful content by imposing a duty of care, requiring highest privacy settings by default, and requiring the provision of parental oversight tools.

The coalition highlighted what it perceives to be improvements to prior drafts of KOSA, including the powers of State AGs to enforce KOSA's duty of care provision. Since the letter, KOSA has again been redrafted to remove state AG enforcement authority over the duty of care provision following concerns raised by advocacy groups that states could censor certain types of information. State AG provisions, which give powers over specific provisions of the bill related to safeguards, disclosures, and transparency requirements, remain generally intact. As of this date, KOSA has not been enacted.

C. State AG Opposition to AI Legislation at the Federal Level

Despite supporting federal legislation relating to children's privacy, State AGs have taken a different approach with respect to AI legislation. Even though State AGs have asserted that artificial intelligence poses new challenges and potential avenues of exploitation—such as the proliferation of non-consensual sexual imagery of minors—State AGs have pushed back against federal AI laws that would preempt state laws or strip the State AGs of their enforcement authority.

Federal efforts to prevent a state-by-state patchwork of AI laws failed in July 2025 when the Senate rejected a proposed 10-year moratorium on state-level AI laws by a vote of 99-1. The proposed moratorium, introduced as part of the One Big Beautiful Bill Act, would have broadly prevented states from imposing regulations on artificial intelligence. 40 State AGs signed a letter opposing the moratorium. The State AGs warned that "a broad moratorium on all state action while Congress fails to act in this area" would be "irresponsible" and "deprives consumers of reasonable protections." They also noted that State-level enforcement is likely the future of AI governance, given Congress's inaction. Likewise, a group of 260 state legislators representing all 50 states urged Congress to reject the moratorium. Now that the moratorium has failed, there has been renewed energy at the state level to regulate AI.

Despite their opposition to the moratorium and other federal legislation that would preempt state law, State AGs have staked out a position that they would support federal legislation that allows them to continue to enforce state laws. A bipartisan coalition of 23 State AGs submitted a comment to the National Telecommunications Information Administration urging the agency to ensure that the State AGs "have concurrent enforcement authority in any Federal regulatory regime governing AI." While the fate of any federal AI legislation is hard to predict, it's clear that many State AGs will not support it if they view it as infringing on their ability to oversee and govern this field—including issues like deepfakes, algorithmic targeting, and synthetic child abuse

imagery.

Looking Forward

Businesses should stay apprised of the evolving environment where federal legislative momentum on privacy (COPPA 2.0/KOSA) coexists with AGs seeking to maintain state autonomy in AI governance. With State AGs aggressively enforcing both areas, businesses face the risk of multi-jurisdictional investigations and litigation under prescriptive laws at the federal and state levels, and under generalist statutes like state consumer protection laws.

Additionally, any eventual AI preemption mandate could reshape enforcement capabilities, and might provoke new litigation or multi-state lobbying efforts.

Understanding this bipartisan push and dual federal-state regulatory front is essential for anticipating legal risks and developing holistic compliance strategies.

Gibson Dunn's State AG Task Force assists clients in responding to subpoenas and civil investigative demands, interfacing with state or local grand juries, representing clients in civil and criminal proceedings, and taking cases to trial.

[1] "Youth" or "child" means individuals under age 18 unless otherwise noted.

[2] 2024 N.Y. Laws ch. 120.

[3] Tex. H.B. 18, 88th Leg., R.S. (2023).

[4] For a comprehensive review of updates to the COPPA Rule, see our client alert FTC Updates to the COPPA Rule Impose New Compliance Obligations for Online Services That Collect Data from Children.

[5] *See* Adjustments to Civil Penalty Amounts, 90 Fed. Reg. 5580 (Jan. 17, 2025) (to be codified at 16 C.F.R. pt. 1). The FTC annually adjusts the civil penalty amount applicable to COPPA violations based on inflation, pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015. *See* Press Release, Fed. Trade Comm'n, FTC Publishes Inflation-Adjusted Civil Penalty Amounts for 2024 (Jan. 11, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-publishes-inflation-adjusted-civil-penalty-amounts-2024. Accordingly, civil penalty violation amounts will rise in future years.

The following Gibson Dunn lawyers prepared this update: Ashlie Beringer, Theodore J. Boutrous, Keith Enright, Nicola T. Hanna, Natalie J. Hausknecht, Poonam G. Kumar, Vivek Mohan, Connor S. Sullivan, Eric D. Vandevelde, Sara K. Weed, James L. Zelenay Jr., Jacob

Arber, Zoey Clark, Kate Googins, Alexus Payton Leach, Michael DJ Landell, and Billy Malmed.

Gibson Dunn lawyers are closely monitoring developments and are available to discuss these issues as applied to your particular business. If you have questions, please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any of the following leaders and members of the firm's State Attorneys General (AG) Task Force, who are here to assist with any AG matters:

State Attorneys General (AG) Task Force:

Artificial Intelligence:
Keith Enright – Palo Alto (+1 650.849.5386, kenright@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213.229.7186, evandevelde@gibsondunn.com)

Antitrust & Competition:
Eric J. Stock – New York (+1 212.351.2301, estock@gibsondunn.com)

Climate Change & Environmental:
Rachel Levick – Washington, D.C. (+1 202.887.3574, rlevick@gibsondunn.com)

Consumer Litigation & Products Liability:
Christopher Chorba – Los Angeles (+1 213.229.7396, cchorba@gibsondunn.com)

Consumer Protection:
Gustav W. Eyler – Washington, D.C. (+1 202.955.8610, geyler@gibsondunn.com)
Natalie J. Hausknecht – Denver (+1 303.298.5783, nhausknecht@gibsondunn.com)
Ashley Rogers – Palo Alto/Dallas (+1 214.698.3316, arogers@gibsondunn.com)

DEI & ESG:
Stuart F. Delery – Washington, D.C. (+1 202.955.8515,sdelery@gibsondunn.com)
Mylan L. Denerstein – New York (+1 212.351.3850, mdenerstein@gibsondunn.com)

False Claims Act & Government Fraud:
Winston Y. Chan – San Francisco (+1 415.393.8362, wchan@gibsondunn.com)
Jonathan M. Phillips – Washington, D.C. (+1 202.887.3546, jphillips@gibsondunn.com)
Jake M. Shields – Washington, D.C. (+1 202.955.8201, jmshields@gibsondunn.com)
James L. Zelenay Jr. – Los Angeles (+1 213.229.7449, jzelenay@gibsondunn.com)

Labor & Employment:
Jason C. Schwartz – Washington, D.C. (+1 202.955.8242, jschwartz@gibsondunn.com)
Katherine V.A. Smith – Los Angeles (+1 213.229.7107, ksmith@gibsondunn.com)

Privacy & Cybersecurity:
Ryan T. Bergsieker – Denver (+1 303.298.5774, rbergsieker@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650.849.5203, cgaedt-sheckter@gibsondunn.com)
Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com)

Securities Enforcement:
Osman Nawaz – New York (+1 212.351.3940, onawaz@gibsondunn.com)
Tina Samanta – New York (+1 212.351.2469, tsamanta@gibsondunn.com)
David Woodcock – Dallas (+1 214.698.3211, dwoodcock@gibsondunn.com)
Lauren Cook Jackson – Washington, D.C. (+1 202.955.8293, ljackson@gibsondunn.com)

Tech & Innovation:
Ashlie Beringer – Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com)

White Collar & Litigation:
Collin Cox – Houston (+1 346.718.6604,ccox@gibsondunn.com)
Trey Cox – Dallas (+1 214.698.3256,tcox@gibsondunn.com)
Nicola T. Hanna – Los Angeles (+1 213.229.7269, nhanna@gibsondunn.com)
Allyson N. Ho – Dallas (+1 214.698.3233,aho@gibsondunn.com)
Poonam G. Kumar – Los Angeles (+1 213.229.7554, pkumar@gibsondunn.com)