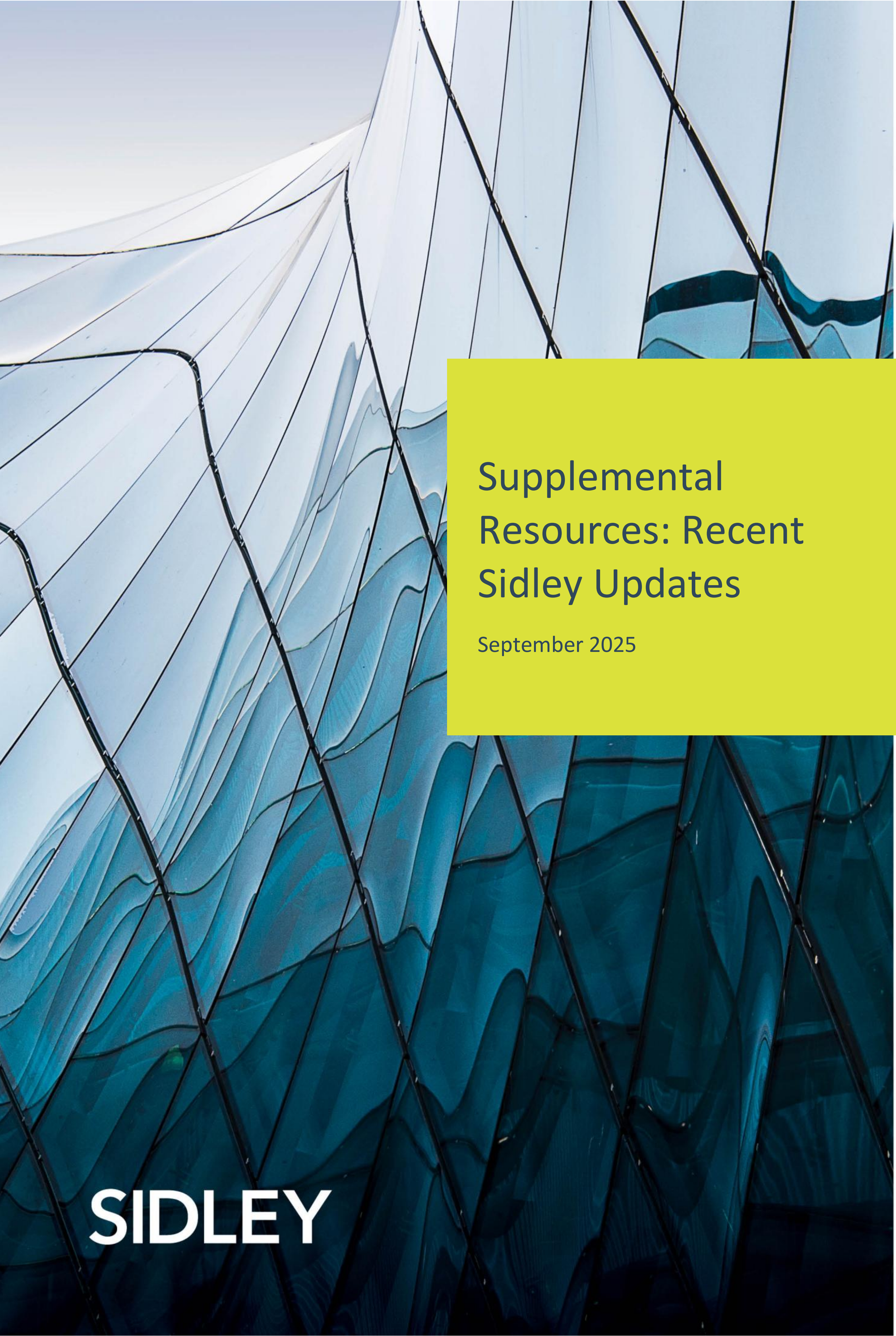

Supplemental Resources: Recent Sidley Updates

September 2025

SIDLEY

TALENT. TEAMWORK. RESULTS.

Table of Contents

Cautionary Reminder: With respect to new matters, an attorney-client relationship between the Company and Sidley Austin LLP will not be created unless and until the Company decides to retain us and an appropriate engagement letter has been signed by each of us. As a result, the Company should refrain from giving us any information the Company would consider privileged or highly confidential until we are retained as the Company's counsel. In addition, lawyers at our Firm may comment on or analyze factual and legal issues involved in the Company's matter to help you assess our suitability for this engagement. Such comments will necessarily be preliminary in nature, and until we are retained by the Company, they should only be used for the purpose of deciding whether to engage us. If we are not retained by the Company, any information you provide to us will not prevent us from representing others in this or any other matter.

The Trump Administration’s 2025 AI Action Plan – Winning the Race: America’s AI Action Plan – and Related Executive Orders

*Originally posted to **sidley.com** on July 30, 2025.*

On July 23, 2025, the Trump administration released its much-anticipated **AI Action Plan**, outlining 90 federal policy positions across three key pillars: Accelerating Innovation, Building American AI Infrastructure, and Leading in International Diplomacy and Security. These pillars are designed to guide near-term action and are underpinned by three cross-cutting priorities: protecting and promoting American workers, ensuring that artificial intelligence (AI) systems are trustworthy and free from ideological bias, and safeguarding AI from misuse, theft, or other risks posed by malicious actors. The scope of the AI Action Plan demonstrates the far-reaching impact of AI, with policy positions affecting not only technology but also trade, national security, cybersecurity, energy, labor, education, **environmental** regulation, antitrust, science, and financial markets.

Accompanying the AI Action Plan were three executive orders. The first promotes the development and export of the “American AI Technology Stack.” The second directs a streamlining of the federal permitting process for building data centers. The third mandates the adoption of “Unbiased AI Principles,” which prioritize “truth-seeking” in response to AI user prompts and “ideological neutrality” in federal government procurement. These executive orders build upon four previous AI-related executive orders issued by President Donald Trump earlier in 2025 as well as two from his first term.

The AI Action Plan follows on President Trump’s January 23, 2025, Executive Order 14179, “Removing Barriers to American Leadership in Artificial Intelligence.” The AI Action Plan was drafted by the White House Office of Science and Technology Policy (OSTP), which coordinated with advisers across the federal government and solicited input from the private sector. The AI Action Plan opens with a quote from President Trump, “As our global competitors race to exploit [a new frontier of scientific discovery], it is a national security imperative for the United States to achieve and maintain unquestioned and unchallenged global technological dominance. To secure our future, we must harness the full power of American innovation.”

Accelerating Innovation

The first pillar, Accelerating Innovation, is designed to ensure that the United States remains at the forefront of AI research, development, and deployment. This involves increasing federal investment in AI research and development, fostering public-private partnerships to develop “secure, full stack AI export packages,” and supporting the commercialization of cutting-edge AI technologies. It also seeks to promote adoption of AI through a variety of measures, including promoting interoperability and leveraging open-source and open-weight AI. The AI Action Plan seeks to “ensure America has leading open models founded on American values.” It further notes that “[o]pen-source and open-weight models could become global standards in some areas of business and in academic research worldwide. For that reason, they also have geostrategic value.” The AI Action Plan further proposes to strengthen export control enforcement to protect American AI innovation and promote the adoption of American AI stacks within a global alliance.

The AI Plan calls for streamlining regulatory pathways to accelerate the introduction of new AI solutions to the market. This principle was also reflected in Vice President Vance’s remarks at the Artificial Intelligence Action Summit in Paris earlier this year. The Trump administration intends to solicit private sector and public input through an OSTP Request for Information (RFI) on federal rules that could be eliminated to help promote AI innovation as well as to review Federal Trade Commission (FTC) investigations initiated under the Biden administration, including final orders and consent decrees.

This focus on deregulation underscores a contrast between the Trump administration, which is emphasizing deregulation, and certain states that are strengthening AI regulation and enforcement. This divergence is particularly salient in light of an unsuccessful attempt to impose a 10-year moratorium on state-level AI regulation in the One Big Beautiful Bill Act, which President Trump signed into law on July 4, 2025. The moratorium, which was initially included in the House version of the bill, was taken out of the Senate version by a near unanimous vote. Relatedly, the AI Action Plan recommends that the White House Office of Management and Budget (OMB) collaborate with federal agencies overseeing AI-related discretionary funding programs to assess the states' AI regulatory environment as part of funding decisions, ensuring that federal resources are not allocated to states with legal regimes deemed to "hinder the effectiveness of such funding."

According to the AI Action Plan, by reducing legal risks and prioritizing support for market-driven innovation, the administration aims to drive economic growth, create high-quality jobs, and maintain America's competitive edge in the global technology landscape.

Building American AI Infrastructure

The second pillar, Building American AI Infrastructure, centers on establishing the physical, digital, and human capital foundations necessary for robust AI development and deployment. This includes modernizing, securing, and expanding data center capacity, enhancing and expanding the power grid, improving American industry's access to high-performance computing resources, and ensuring the availability of secure, high-quality data for AI training and testing. The AI Action Plan also places a strong emphasis on workforce development, with initiatives to encourage the upskilling of American workers and AI education pipelines. This builds on the cyber workforce initiative of the Biden administration.

Security is a central theme throughout the infrastructure proposals, with multiple policy initiatives focused on national and cybersecurity imperatives. The AI Action Plan highlights the dual objectives of enhancing AI infrastructure for geopolitical leadership and protecting against foreign adversary threats. It calls for the establishment of an AI Information Sharing and Analysis Center (AI-ISAC) to facilitate AI threat intelligence sharing. Several initiatives are aimed at developing standards and controls to ensure that American AI is not built with or supported through the supply chain by "adversarial technology that could undermine U.S. AI dominance."

In addition to increased scrutiny of technologies, the AI Action Plan emphasizes the strategic importance of data, stating that "high quality data has become a national strategic asset." The Trump administration intends to develop minimum data quality standards, expand access to federal data, and break down federal data silos. By investing in secure and resilient infrastructure, the administration seeks to provide American innovators with the resources necessary to succeed and to develop AI tools that reflect American values.

Leading in International Diplomacy and Security

The third pillar, Leading in International Diplomacy and Security, acknowledges the global implications of AI and seeks to ensure that the United States shapes international standards amid a rapidly evolving landscape of international AI laws, regulations, and technical standards. The AI Action Plan outlines strategies to promote the adoption of American-developed AI technologies and standards and to leverage America's global leadership in technology to forge "an enduring global alliance." The AI Action Plan promotes exporting America's "full AI technology stack — hardware, models, software applications and standards — to all countries willing to join

America’s AI alliance.” The AI Plan also warns that “the failure to meet this demand would be an unforced error, causing these countries to turn to our rivals.”

Pillar III includes measures to encourage allies to implement export controls aligned with the U.S. regime, thereby protecting American AI intellectual property and preventing the export of sensitive technologies to adversaries. These efforts are also intended to bolster the cybersecurity and resilience of critical infrastructure against AI-enabled threats. The AI Action Plan further proposes initiatives to refine American standards, including a review of the globally recognized National Institute of Standards & Technology (NIST) AI Risk Management Framework. The Trump administration aims to ensure that AI advances serve the interests of the United States and its allies, reflect the administration’s priorities and values, and mitigate risks associated with the misuse or weaponization of AI.

Developments to Come

As emphasized in President Trump’s preamble and throughout the three pillars, the Trump administration’s 2025 AI Action Plan is focused on promoting American technology dominance. While the AI Action Plan identifies extensive policy positions in a variety of areas, we expect the Administration’s AI strategy will continue to evolve in an effort to keep pace with AI’s warp-speed evolution.

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**
Michael E. Borden, Partner	+1 202 736 8521, **mborden@sidley.com**
Jen Fernandez, Partner	+1 202 736 8824, **jen.fernandez@sidley.com**
Sharon R. Flanagan, Partner	+1 415 772 1271, **sflanagan@sidley.com**
Michael Hochman, Partner	+1 202 736 8470, **michael.hochman@sidley.com**
David C. Lashway, Partner	+1 202 736 8059, **dlashway@sidley.com**

A Mid-Year Privacy Check-In – Important Developments and New Compliance Obligations for Privacy Laws

*Originally posted to **Data Matters** on July 31, 2025.*

During the first half of 2025, state legislators and regulators have been working overtime to enact new data privacy laws and expand existing laws, all of which are likely to have an impact on businesses in the remainder of the year and into 2026. These efforts reflect key themes such as increased regulation of teen data and social media platforms, enhanced restrictions on the collection and sale of geolocation and biometric data, simplified opt-out mechanisms for tracking technologies, and broader obligations concerning consumer health data and data minimization. In parallel, significant regulatory activity surrounding AI has emerged, including a new federal AI Action Plan and proposed amendments to the CCPA addressing automated decision making technologies, alongside a wave of new state AI laws.

Beyond tackling new subject areas, lawmakers have expanded the scope of existing legislation. This includes lowering thresholds of applicability, removing exemptions for specific entity types broadly subject to federal privacy laws such as the Gramm-Leach-Bliley Act (GLBA).

Enforcement activity has continued apace. California regulators have issued several instructive enforcement actions within the last six months, focusing on the need to audit cookie classifications, pressure test opt-out links, and scrutinize the user experience as consumers exercise their privacy rights. The California Privacy Protection Agency is also beginning to focus on purpose limitations in CCPA regulations, in particular as they relate to sensitive data uses. Enforcement reports from state attorneys general mirror these concerns and stress the importance of clear privacy policy disclosures that clearly apprise state residents of their rights.

Industry pushback against aggressive state legislation has seen mixed results. Litigation in federal court around laws seeking to protect children online has led to some state laws being upheld, and some struck down, leaving a complex landscape for age verification standards and age-appropriate design code initiatives. Also unsuccessful, at least this year, was an effort by some California legislators to clarify the scope of the state's wiretap law (CIPA) in a manner that would have put an end to the "shakedown" lawsuits and demand letters hitting businesses of all sizes for common and even purely operational website functionality. On the other hand, industry (and California legislative) efforts to rein in some of the more aggressive elements of proposed CCPA AI regulations appear to have succeeded, as proposed rules making their way through the final stages of rulemaking were significantly scaled back from initial drafts. (For more information about recent CCPA rulemaking, see Sidley Data Matters – California Privacy Protection Agency Advances Substantial Rulemaking – Cyber Audits, Risk Assessments, New Automated Decision making Rights, and More). At the federal level, efforts to place a moratorium on enforcement of the growing patchwork of state AI laws also failed—which may further bolster the trend of state AI legislation.

These developments unfold within a broader legal landscape already defined by close to two dozen state privacy laws—some newly effective in 2025 and others becoming effective later this year and in January 2026.

Notable Trends – Mid Year 2025

I. Children and Teen Privacy and Online Protection

Several states have enacted strict laws targeting the collection and sale of minors' data. Key provisions vary by state and include:

- Opt-in consent for the collection of teens' data unless reasonably or strictly necessary to provide a service or product (e.g., NY, CO, MT);
- Opt-in consent for the sale of teen data or its use for targeted advertising (e.g., CO, NY);
- Complete bans on targeted advertising or sale of teen data, regardless of consent (e.g., OR); and
- Prohibitions on the sale of geolocation data (e.g., LA [for social media platforms], MD [all ages]).

In addition, Colorado has initiated rulemaking to define what constitutes "willful disregard" in determining a user's minor status, and how service design features might increase or sustain a minor's use of an online service, potentially in violation of provisions of Colorado's privacy law regarding minors' data. The state's amendments apply even to businesses that don't meet the general CPA thresholds, but make products or services available in Colorado—an approach also adopted by Montana and Oregon.

The impact of app store age-verification laws, scheduled to take effect in 2026, could be significant. These laws would require app stores to verify users' ages and then send signals to app developers indicating users' age ranges, with some variation by state. In addition to triggering compliance obligations under state data privacy laws, knowing the age of app users may also implicate compliance with the federal Children's Online Privacy Protection Act (COPPA), including new regulations finalized earlier this year that, among other things, institute new consent requirements for digital advertising, written information security programs, and more requirements that will be enforceable beginning in April 2026.

II. Service Providers and Third Parties: Expanded Requirements and Regulator Expectations

States are increasingly requiring transparency around third-party data sharing. For example:

- Minnesota's new data privacy law, effective July 31, 2025, grants residents the right to know the identities of third parties receiving their data—mirroring requirements under Oregon's law and pending changes in Connecticut's law that will become effective July 1, 2026.
- New COPPA rules require entities to disclose, in their online privacy notices, the identities and categories of third parties to which an operator (an entity subject to COPPA) discloses children's personal data.
- Regulators in California have signaled their expectation that businesses maintain comprehensive inventories of vendors that process or otherwise receive personal data to ensure appropriate contractual terms required by the CCPA are in place.
- The Department of Justice's recently enacted Data Security Program requirements under Executive Order 14117 Preventing Access to Americans' Bulk Sensitive Personal Data also highlights the importance of vendor diligence.
- Lawsuits focused on the use of third-party website technologies are also on the rise.

III. Sensitive Data: Biometric, Sexual Health, and Location Data

Several states have enacted laws concerning sensitive data types, and one bill addressing this topic is still pending:

- Colorado now mandates opt-in consent for sharing/selling biometric data and requires annual retention reviews—even if biometric identifiers are not used to identify individuals. As previously reported, this amendment to the Colorado Privacy Act applies more broadly than other provisions of the law with data thresholds and instead applies to all companies doing business in Colorado or that otherwise make their products or services available in the state.

- Virginia, via its Consumer Protection Act (separate from the Virginia Consumer Data Protection Act (VCDPA)) now requires opt-in consent for collecting, selling, or disclosing "reproductive or sexual health" data in connection with consumer transactions, including advertising. This definition is broader than a similar term used in Virginia's data privacy law, including because it includes derived/inferred data. Notably, this law includes a private right of action and applies more broadly than the VCDPA to all de
- Location data restrictions: States have continued to strengthen laws concerning the collection and processing of precise location data. For example, Colorado requires opt-in consent and disclosure when collecting teen geolocation data. Oregon and Maryland have imposed outright bans on sales of geolocation data. A proposed CCPA amendment (AB-322) includes a similar ban on the sale of such data and would also prohibit the leasing or "trading" of such data.

IV. Revisions to Applicability Thresholds and Exemptions

Several states have amended their state data privacy laws to expand their scope, including:

- Lowered applicability thresholds:
  - Montana: From 50,000 to 25,000 residents' data.
  - Connecticut: From 100,000 to 35,000 residents' data; no thresholds for entities that engage in the sale of personal data or that control or process sensitive data (unless used to process payments). Sensitive data definitions were also expanded and will include, for example, biometric data even if not used to identify an individual; financial account log-in or credit card or debit card with access codes or passwords that allow access; and government-issued ID numbers.
- GLBA exemptions narrowed:
  - Amendments to laws in Connecticut and Montana exempt only GLBA-covered data and certain types of financial institutions—not every type of entity subject to GLBA.
- Nonprofit exemptions refined:
  - In Montana, nonprofits are now mostly in scope—except those focused on insurance fraud prevention.

Looking Ahead

This mid-year update highlights some of the most important U.S. state privacy developments, with more changes anticipated in the second half of 2025. Privacy enforcement remains a high priority among state AGs and regulators, with additional interpretive guidance likely to emerge. It will be important for businesses to stay vigilant and proactively review their privacy programs for compliance in this rapidly evolving landscape.

CONTACTS

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

Colleen Theresa Brown, Partner	+1 202 736 8465, ctbrown@sidley.com
Sheri Porath Rockwell, Counsel	+1 310 595 9512, sheri.rockwell@sidley.com
Sasha Hondagneu-Messner, Managing Associate	+1 212 839 5403, shondagneumessner@sidley.com

California Privacy Protection Agency Advances Substantial Rulemaking – Cyber Audits, Risk Assessments, New Automated Decisionmaking Technologies Rights, and More

*Originally posted to **Data Matters** on July 29, 2025.*

The California Privacy Protection Agency (Agency) on Thursday, July 24, 2025, approved a comprehensive set of new California Consumer Privacy Act (CCPA) regulations that the Agency has been developing for over four years. Before taking effect, the proposed regulations must still be approved by California's Office of Administrative Law (OAL). It is possible some of these provisions may change with the OAL's review, which must be completed within 30 business days after the Agency submits to the OAL its final rulemaking package. However, many expect that most of the proposed regulations will pass OAL review. If approved, several of the proposed regulations would be effective as of January 1, 2026. Key requirements under the proposed regulations include:

- **Annual Independent Cyber Audits:** Certain businesses would be required to undergo annual independent cybersecurity audits, with a phased implementation from 2027 to 2029 as discussed in greater detail below. These audits would include executive reporting and sworn certification requirements.
- **Detailed Risk Assessment Requirements:** Businesses would need to conduct risk assessments for activities such as the sale and sharing of personal information (as defined by the CCPA), processing of sensitive data, profiling in for-profit educational and employment contexts, and the training of automated decisionmaking technologies (ADMT) used to make "significant decisions" (including those related to finance, lending, housing, for-profit educational enrollment, employment, and healthcare services). These risk assessments would also require senior management reporting.
- **New Rights for Consumers Related to ADMT:** Beginning in 2027, there would be new notice, access, and opt-out rights for individuals regarding the use of ADMT in making significant decisions.

Additionally, the proposed regulations would update some existing CCPA requirements. Notable changes could include:

- **Consumer Notification:** Businesses would be required to notify consumers when Global Privacy Control (GPC) and other opt-outs are in effect.
- **Dark Pattern Prohibitions:** The proposed regulations provide further guidance and warnings with respect to the use of dark patterns in the design of opt-out requests and consent mechanisms, such as cookie banners, reflecting recent CCPA enforcement trends.

Several of the proposed regulations would be phased in over time, while other provisions could take effect as early as January 1, 2026, depending upon the timing and scope of OAL approval. All businesses subject to the CCPA should carefully review the proposed regulations to determine their applicability and begin planning for implementation. This may include budgeting for increased compliance costs, such as ongoing cybersecurity audits and risk assessments.

While a comprehensive review of the many substantive provisions of these proposed regulations is beyond the scope of this summary, we highlight below some of the more notable features:

Mandatory Annual Cyber Audits for Certain Businesses Beginning in 2027

Under the proposed regulations, beginning in 2027, CCPA businesses that meet the following thresholds would be required to undertake annual cybersecurity audits: businesses that (a) annually process the personal information of more than 250,000 California residents; (b) annually process the sensitive personal information of more than 50,000 California residents; and (c) derive more than 50% of their annual revenue from the sale or CCPA-defined sharing of personal information. Once a business falls within any of these thresholds, under the proposed regulations, it must prepare for near-continuous, year-long audit activities. Each audit cycle would culminate in an annual certification, due by April 1, attesting to the accuracy and independence of the audit. This certification would need to be made by a member of the business's executive management team responsible for audit compliance.

Cyber Audit Scope and Process. The proposed regulations would require cybersecurity audits to comprehensively assess the establishment, maintenance, and implementation of a business's cybersecurity program over a 12-month period, beginning January 1 of each year. Audits would need to be conducted by independent assessors using recognized audit frameworks. Auditors would be tasked with evaluating 18 components of the business's cybersecurity program, as applicable, including: inventories of personal information and information systems; multifactor authentication (MFA); access controls; encryption practices; oversight of vendors, service providers, contractors, and third parties; secure code development and testing; and use of internal or external vulnerability scans and penetration testing. Following the assessment, auditors would produce a gap analysis, a remediation plan with target dates, updates on the status of prior years' remediation plans, and identify individuals within the business responsible for cybersecurity.

Phased Implementation Based on Revenue. The proposed regulations would phase in the audit requirement over three years, based on a business's annual gross revenue:

- Businesses with annual revenue over $100 million would need to begin audits by January 1, 2027;
- Businesses with annual revenue between $50 million and $100 million would need to begin audits by January 1, 2028; and
- Businesses with annual revenue under $50 million would need to begin audits by January 1, 2029.

Implications for Businesses. Assuming these regulations are approved by the OAL, compliance costs for businesses of all sizes can be expected to rise. Additionally, the creation of detailed audit records and executive attestations could introduce new areas of legal risk, such as by supporting increased regulatory scrutiny or litigation risks, particularly for businesses that have not previously been subject to independent audit obligations. Careful planning and resource allocation will be essential should these regulations be approved by the OAL.

Detailed Risk Assessments With Annual Reporting Requirements

The proposed regulations would introduce comprehensive requirements for businesses to conduct risk assessments, with California incorporating standards that are not typically seen in other state risk assessment requirements. While, like other state privacy laws, risk assessments would be required for the sale and sharing of personal information (such as the use of advertising trackers and disclosures for cross-context behavioral advertising) and for the processing of sensitive data, proposed regulations would expand the scope significantly. Under the proposed regulations, businesses would also be required to conduct risk assessments for:

- The use of ADMT to make significant decisions about individuals;
- Profiling in employment and educational contexts;
- Profiling based on geolocations designated as "sensitive"; and
- Processing personal information to train ADMT used for significant decisions or to train technologies for identity verification or profiling of California residents, including the advertising or marketing of plans to do so.

Unique California Standards and Focus on "Negative Impacts." California's proposed ADMT regulations detail the factors businesses would need to consider in risk assessments, which could set a standard that is unique among state privacy laws. Notably, instead of focusing solely on the "risks" to consumers, as is common in other states, the proposed regulations would require businesses to evaluate the potential "negative impacts" to consumer privacy. The proposed regulations include several examples of potential negative impacts that a business may consider, including:

- Data security risks
- Discrimination based on protected classes
- Economic harm
- Physical harm
- Reputational harm
- Psychological harm
- Impairing consumers' control over their personal information, such as by not providing consumers with sufficient information to make an informed decision or by interfering with consumers' ability to make choices consistent with their reasonable expectations
- Compelling consumers to allow the processing of personal information, such as by conditioning consumers' acquisition or use of an online service upon their disclosure of personal information that is unnecessary for the expected functionality of the service, or purporting to obtain consent through dark patterns

The latter examples reflect themes seen in recent CCPA enforcement actions and suggest areas where businesses may want to consider focusing their current compliance efforts.

Timing and Reporting Requirements. Risk assessments would be required to be conducted before engaging in any in-scope processing activities and reviewed and updated at least every three years, or within 45 days of a material change in the processing activity. For new processing activities, assessments would be required as soon as the regulations take effect (potentially January 1, 2026). For ongoing activities as of the effective date of the proposed regulations, businesses would be required to complete risk assessments by December 31, 2027.

Importantly, this latest version of the proposed regulations removed the requirement to submit all risk assessments to the Agency. Instead, the proposed regulations would require a senior executive to submit an annual certified report to the Agency, detailing the number and types of risk assessments conducted and the categories of personal information involved. However, the Agency and the California Attorney General would retain the authority to require production of any risk assessment with 30-days' advance notice.

Implications for Businesses. The proposed risk assessment regulations would represent a significant expansion of risk assessment obligations currently in effect under other state privacy laws, both in terms of scope and the factors to be considered. If the proposed CCPA regulations are approved by OAL, businesses will need to further develop robust processes for identifying in-scope activities, conducting and documenting risk assessments, and ensuring timely reporting and updates. The focus on "negative impacts" and the detailed reporting obligations underscore the importance of integrating these assessments into broader CCPA compliance programs and preparing for potential regulatory scrutiny.

New Rights and Obligations for "Significant Decisions" Made With ADMT

The proposed regulations, while scaled back from expansive earlier proposals, would nonetheless establish important new rights for consumers and corresponding obligations for businesses that utilize ADMT to make "significant decisions," a defined term in the proposed regulations that includes decisions related to financial or lending matters, housing, for-profit educational enrollment, employment, and healthcare services—provided that the personal information involved is not otherwise exempt from the CCPA (for example, information subject to the Gramm-Leach-Bliley Act or HIPAA).

A key clarification in the proposed regulations is the definition of ADMT. A technology would only qualify as an ADMT if the technology replaces or "substantially replaces" human decisionmaking. If a human reviews the output of the technology and retains the authority to make or alter the decision, the technology is not an ADMT as defined by the proposed regulations. This clarification was included in response to concerns raised by businesses and industry groups during the rulemaking process. Importantly, the proposed regulations clarify that "significant decisions" for the purposes of ADMT rights do not include advertising directed at consumers.

Under the proposed regulations, businesses that utilize ADMT to make significant decisions would need to address a host of new consumer rights by April 1, 2027. These include issuing a Pre-use Notice at or before the point at which a business collects personal information that will be processed using ADMT. Proposed regulations contemplate that the Pre-use Notice would describe specific purposes for which a business wants to use ADMT, information about how the ADMT works to make decisions, and apprise the consumer of their rights regarding the ADMT, including rights to access and opt out of the use of ADMT. The access right in the proposed regulations would require businesses to provide information about how a consumer's personal information was processed by ADMT and include a description of the logic used by the ADMT, enabling the consumer to understand how their data was analyzed and how the output was generated. The proposed ADMT access right would also require businesses to explain how the ADMT arrived at the decision, including the role of any human involvement in the process. In addition, the proposed regulations include a right for consumers to opt out of the use of ADMT for significant decisions affecting them.

This version of the proposed regulations, particularly the narrowed definition of ADMT, has drawn criticism from some labor groups. Their primary concern is that exempting decisions where humans can override automated outputs may leave workers vulnerable to adverse impacts from automated systems. Agency board discussions and earlier drafts of the regulations indicate that some staff members share these concerns. As a result, it is expected that the use of ADMT in employment and workplace contexts will be subject to heightened regulatory scrutiny going forward.

Implications for Businesses. Businesses that rely on ADMT for significant decisions may want to consider preparations to comply with proposed regulations. Preparations could include cataloging uses of in-scope ADMT, developing clear and transparent Pre-use Notices, establishing processes to provide meaningful access to information about ADMT logic and decisionmaking, and designing mechanisms for consumers to exercise their opt-out rights. Special attention should be paid to workplace applications of ADMT, as these are likely to be a focus of enforcement and regulatory oversight.

Strengthened Opt-Out Notification Requirements and Dark Pattern Reminders

The proposed regulations also reinforce California regulators' ongoing focus on ensuring that consumers can easily understand and exercise their CCPA rights, with a particular emphasis on opt-out rights.

Under the proposed regulations, businesses would need to display on their websites whether they have processed Global Privacy Control (GPC) signals as valid opt-out requests. Additionally, when processing sale or share opt-out requests made through a website or app, businesses would need to provide a mechanism for consumers to confirm their opt-out request has been honored. Consent management platforms can be expected to play a key role in facilitating compliance with these proposed requirements; indeed, some platforms already offer such functionality.

Implementing these measures contemplated by the proposed regulations have the potential to expose potential compliance gaps in how businesses process opt-out signals. Common issues include inconsistent transmission of opt-out signals across different webpages and challenges in recognizing authenticated account holders across multiple devices. These shortcomings can create both regulatory and litigation risks, as plaintiffs' lawyers have increasingly focused on purportedly ineffective opt-out mechanisms to allege privacy violations. These risks may be further heightened if the California Opt Me Out Act (AB 566)—which would require all browsers to recognize GPC signals—is enacted. This would likely increase the volume of GPC signals that businesses must process.

The proposed regulations would also strengthen requirements around the design of opt-out requests and consent mechanisms with emphasis on providing symmetrical and clearly worded choices. This reflects the recent enforcement priorities of both the Agency and the California Attorney General. The proposed regulations further clarify that simply navigating away from a page or dismissing a pop-up banner does not, by itself, constitute valid consent. This language mirrors similar provisions in Colorado's privacy regulations.

Implications for Businesses. In light of these proposed changes to CCPA regulations, businesses may wish to consider proactively testing their systems for processing GPC signals and other opt-out requests—potentially through third-party audits—in advance of the anticipated January 1 effective date of several of the proposed regulations and, if enacted, the California Opt Me Out Act. Businesses should also consider reviewing and, if necessary, updating the design and language of their opt-out features and cookie banners, benchmarking them against the numerous examples provided in section 7004 of the proposed CCPA regulations.

CONTACTS

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

Colleen Theresa Brown, Partner	+1 202 736 8465, ctbrown@sidley.com
Thomas D. Cunningham, Partner	+1 312 853 7594, tcunningham@sidley.com
Sheri Porath Rockwell, Counsel	+1 310 595 9512, sheri.rockwell@sidley.com
Sasha Hondagneu-Messner, Managing Associate	+1 212 839 5403, shondagneumessner@sidley.com
Stephanie Y. Lim, Associate	+1 212 839 8529, stephanie.lim@sidley.com

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

*Originally posted to **sidley.com** on 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 unfair 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.

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

SIDLEY