New US Obligations for New Technology: Cybersecurity and Data Privacy Predictions for the Remainder of 2025

As rapid technological advances create new challenges to security and privacy interests, US companies and other entities that obtain, use, or disclose consumer, employee, or government data face an ever-growing web of legal and regulatory obligations. The complexity will only compound as new artificial intelligence laws and regulations interact with existing requirements for the capture, storage, and transfer of data.

We anticipate that the remainder of 2025 will bring significant developments in four crucial domains: (1) state artificial intelligence laws, (2) updated state data privacy laws, including new comprehensive statutes, (3) increased federal enforcement of cybersecurity reporting regulations and compliance with cybersecurity standards included in federal contracts, and (4) stricter international data privacy laws, including new private rights of action and data transfer protocols. Companies should review their policies and procedures to ensure they remain in compliance with the developments outlined below.

Artificial Intelligence: States Take the Lead

We anticipate that artificial intelligence and automated decision-making technology will remain a focus of regulatory and legislative efforts, primarily at the state level. At the federal level, President Trump revoked President Biden's 2023 Executive Order on AI[1] and implemented a new executive order, "Removing Barriers to American Leadership in Artificial Intelligence."[2] US policy, as stated in the Trump EO, is to "sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security." Additionally, in late July 2025, the Trump administration released a comprehensive AI Action Plan, "Winning the Race: America's AI Action Plan," and issued three executive orders aimed at accelerating American AI innovation, streamlining infrastructure development, and promoting US AI technologies abroad. The Action Plan and accompanying executive orders emphasize federal deregulation and promoting open-source AI development.[3]

In addition, the US Cybersecurity and Infrastructure Security Agency (CISA) recently issued in May 2025 new cybersecurity guidelines, in collaboration with the National Security Agency (NSA) and the

[1] Exec. Order No. 14,110 (2023).

[2] Exec. Order No. 12,179 (2025).

[3] *Winning the Race: America's AI Action Plan*, The White House (July 2025) available at https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

Federal Bureau of Investigation (FBI). The Cybersecurity Information Sheet, titled "AI Data Security: Best Practices for Securing Data Used to Train and Operate AI Systems," emphasizes the need for data protection in AI to ensure its accuracy and integrity as AI becomes more intertwined with critical infrastructure. The Information Sheet focuses on best practices for data security via regulation throughout the AI lifecycle, although it primarily addresses strategies at the corporate, as opposed to state, level.

Despite the Trump administration's AI Action Plan and considering that new comprehensive federal regulations seem unlikely in the short term, and Congress failed to include a proposed moratorium in the recent reconciliation package of the One Big Beautiful Bill, we expect states to take the lead on AI-related legislative and regulatory efforts in the second half of 2025. The following are some of the pending bills and regulations that could take effect in the near future:

California: The California Privacy Protection Agency (CPPA) has developed rules that would require businesses to provide consumers a pre-use notice and allow them to opt out of and obtain access to information about automated decision-making technology (ADMT), including ADMT involving AI. The proposed regulations apply to the use of ADMT for decisions with important consequences for consumers (such as financial services, housing, educational or employment opportunities, and essential goods or services). Additionally, the regulations address the use of personal information to train ADMT.[4] On July 24, 2025, the CPPA submitted the proposed rules to the California Office of Administrative law for approval before they take effect.

Connecticut: Legislators in Connecticut pursued sweeping AI regulation in last year's proposed SB-2. The bill's private sector provisions regulated both developers and deployers of AI systems. It required those who develop or deploy "high-risk" AI models that make, or that may be a substantial factor in making, certain material decisions to use reasonable care in preventing algorithmic discrimination. SB-2 also sought to impose substantial risk management and disclosure requirements on the development and use of AI, including the known or reasonably foreseeable risks of the AI system, a summary of data used in the training of the AI system, and the nature and use of AI decision-making in a given business.[5] While the Connecticut Senate passed SB-2, political backlash prevented the bill from being heard in the House of Representatives. Proponents of AI regulation have introduced an updated SB-2 for this 2025 session.[6]

---

[4] *Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decision-making Technology (ADMT), and Insurance Companies*, California Privacy Protection Agency (last accessed Aug. 1, 2025) available at https://cppa.ca.gov/regulations/ccpa_updates.html.

[5] Connecticut S.B. No. 2 (2024) available at https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00002&which_year=2024.

[6] *See* Michelle Rappaport, *Senate Democrats to Prioritize AI Regulation in 2025 Session, Connecticut State Democrats*, Capital Dispatch (Dec. 23, 2024) available at https://www.senatedems.ct.gov/senate-democrats-to-prioritize-ai-regulation-in-2025-session. Track progress here of the updated SB-2: https://www.cga.ct.gov/asp/CGABillStatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB2.

Colorado: On May 17, 2024, Colorado enacted the Colorado Artificial Intelligence Act (CAIA), aimed at regulating "high-risk" AI systems. Effective February 1, 2026, the CAIA requires both developers and deployers of high-risk AI systems to use reasonable care to protect consumers from algorithmic discrimination based on protected characteristics. Companies utilizing high-risk AI systems must notify consumers when a high-risk AI system is used to make a consequential decision about them, provide information about the system and its impact, and offer opportunities for consumers to correct data, appeal adverse decisions, and request human review. The CAIA is enforced exclusively by the Colorado Attorney General, with no private right of action.[7]

Massachusetts: State lawmakers are currently considering H.94, the Artificial Intelligence Accountability and Consumer Protection Act. Under the proposed bill, developers of AI systems must actively identify, mitigate, and disclose risks of algorithmic discrimination, provide notice to the state Attorney General upon discovery of a known or foreseeable risk of algorithmic discrimination, and publicly disclose, via a developer's website, information about the type of AI system developed and measures taken to prevent discrimination. Corporations using AI systems to target consumers or otherwise influence consumer behavior would be required to disclose such efforts through publication on the corporation's website. The bill would mandate that any deployer of a "high-risk" AI system implement risk management policies, conduct impact assessments, and disclose the AI system in use and the risk management strategies in place.[8]

New Mexico: Legislators in New Mexico are considering HB 60, the Artificial Intelligence Act, which would impose a duty of care on developers of AI systems to prevent algorithmic discrimination and disclose known and foreseeable risks of harm. For deployers of AI systems, HB 60 requires the development of a risk management policy and a schedule of impact assessments. When incidents of algorithmic discrimination are discovered, HB 60 mandates that developers and deployers notify New Mexico's Department of Justice. Both the Justice Department and consumers may enforce the act and, in the case of the consumer, receive attorneys' fees for any violation.[9]

New York: In October 2024, the New York Department of Financial Services (NYDFS) issued guidance on Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks. While the guidance does not impose any additional requirements, it does provide recommendations to covered entities under the NYDFS Cybersecurity

[7] Colorado, SB24-205 (2024) available at https://leg.colorado.gov/bills/sb24-205. Recently, the CAIA has received pushback from various stakeholders and Colorado Governor Polis has expressed interest in calling a special legislative session to consider changes to the CAIA. *See Colorado Governor Polis Orders Legislature Back to Change AI Law,* Bloomberg Law available at (https://news.bgov.com/bloomberg-government-news/colorado-gov-polis-orders-legislature-back-to-change-ai-law) (Aug. 6, 2025).

[8] Massachusetts, H.94 (*An Act to Ensure Accountability and Transparency in Artificial Intelligence Systems*) (2025) available at https://malegislature.gov/Bills/194/HD396.

[9] New Mexico HB 60, Artificial Intelligence Act (2025), available at https://www.nmlegis.gov/Legislation/Legislation?chamber=H&legtype=B&legno=60&year=25.

Regulation for addressing these risks, including those related to AI-enabled social engineering (such as deepfakes), AI-enhanced cybersecurity attacks, large quantities of AI-processed data, and third-party AI-powered tools. The NYDFS recommends that covered entities adopt controls to address and manage those risks, including risk-based programs, policies, procedures, and plans; third-party service provider and vendor management controls; and cybersecurity training, monitoring, and data management.[10]

New York is also considering a law (AB A3356) that would require registration and licensing of high-risk, advanced artificial intelligence systems and impose certain requirements and an ethical code of conduct on their use.[11] New York lawmakers have already passed the Responsible AI Safety and Education Act (RAISE Act), which would impose obligations on developers of large "frontier" AI models—a model trained with more than US$100 million in computation costs or that exceeds a specified computational threshold. The RAISE Act is designed to prevent "critical harm" caused by or materially enabled by advanced AI systems, including mass casualty events or at events that garner at least US$1 billion in damages. Under the Act, developers must implement and maintain written safety and security protocols, retain unredacted copies of these protocols for the duration of model deployment plus five years, and publish a redacted version for public transparency. The RAISE Act would be enforced by the New York Attorney General, with penalties of up to US$10 million for a first violation and US$30 million for subsequent violations, and does not provide a private right of action.[12]

Texas: On June 22, 2025, Texas enacted HB 149, the "Texas Responsible Artificial Intelligence Governance Act." Effective as of January 1, 2026, the act aims to prevent any individual or entity from developing or deploying AI systems for illegal or harmful purposes, including intentionally causing harm, engaging in criminal activity, unlawfully discriminating against protected classes, or infringing on constitutional rights. Enforcement authority is vested exclusively in the Texas Attorney General; there is no private right of action, but the Attorney General is required to create and maintain an online portal for consumers to submit complaints.[13]

Virginia: Virginia lawmakers have already considered numerous bills related to AI regulation that spotlight where future regulation may be headed. HB2094, the High-Risk Artificial Intelligence Developer and Deployer Act, aimed to set operating standards for AI development and deployment to ensure transparency in consequential decision-making and

[10] Industry Letter, New York Department of Financial Services (Oct. 16, 2024) available at https://www.dfs.ny.gov/industry-guidance/industry-letters/il20241016-cyber-risks-ai-and-strategies-combat-related-risks.

[11] New York Assembly Bill A3356 (2025) available at https://www.nysenate.gov/legislation/bills/2025/A3356.

[12] New York Assembly Bill A6453A (2025) available at https://www.nysenate.gov/legislation/bills/2025/A6453/amendment/A.

[13] Texas HB 149 (2025) available at https://capitol.texas.gov/BillLookup/History.aspx?LegSess=89R&Bill=HB149.

to impose civil penalties for failing to protect consumers from algorithmic discrimination.[14] The Digital Content Authenticity and Transparency Act, HB2121, would require developers of AI systems to implement data protocols and transparency measures to track and disclose the creation of synthetic digital content.[15] And while stalled in committee, HB2250, the Artificial Intelligence Training Data Transparency Act, would allow AI consumers to opt out of personal data use through notification to a third party (such as a web-browsing application) and would also establish a broad requirement to disclose the information an AI system was or is being trained on.[16]

Given the scope of the proposed state AI legislation described above, companies should carefully account for and review their use of AI and, if not already in place, develop comprehensive policies and procedures in consultation with both internal stakeholders and outside counsel to meet emerging standards for risk management and expanded consumer rights.

State Privacy Law: An Expansion of Consumer Rights

Numerous states made critical changes to their privacy laws in 2024, from updating state privacy regulations to passing new, comprehensive privacy statutes. California, for instance, enacted regulations tightening restrictions on data brokers and announced a new set of proposed regulations covering automated decision-making and other topics. Many other states took legislative action on privacy, whether passing new privacy laws—both comprehensive and sector-specific—or amending existing statutes. In all, 2024 was another year of significant privacy-law expansion and adaptation, with yet more changes coming in 2025.

California Privacy Protection Agency Regulations

The California Privacy Protection Agency (CPPA) took major actions to expand the state's privacy regulations in 2024.

In November 2024, the CPPA gave final approval to revised regulations governing data brokers. The changes broadened the definition of "data broker" by including businesses that have "a direct relationship with a consumer but also sell[] personal information about the consumer that the business did not collect directly from the consumer." This change may result in many more businesses now being considered data brokers under the California Consumer Privacy Act (CCPA). Other changes included a large hike, from US$400 to US$6,600, in the annual fee required to

[14] Virginia HB2094, High-Risk Artificial Intelligence Developer and Deployer Act (2025) available at https://lis.virginia.gov/bill-details/20251/HB2094.
On March 4, 2025 Governor Youngkin vetoed HB2094 and on April 2, 2025, the Virginia House of Representative sustained the Governor's veto.

[15] Virginia HB2121, Digital Content Authenticity and Transparency Act (2025) available at https://lis.virginia.gov/bill-details/20251/HB2121. Note, this bill has been left in committee and is unlikely to move forward.

[16] Virginia HB2250 (2025) available at https://lis.virginia.gov/bill-details/20251/HB2250. Note, this bill has also been left in committee and is unlikely to move forward.

register as a data broker in California. The changes took effect December 27, 2024. Data brokers were obligated to collect and report specific information by July 1, 2025. The California Privacy Protection Agency is expected to continue enforcement and add further requirements in the coming years. By August 1, 2026, data brokers must access the accessible deletion mechanism, which allows consumers to request deletion of personal information, at least once every 45 days and process deletion requests.[17]

That same month, the CPPA announced a proposed rulemaking that would make several amendments to the state's privacy regulations.[18]

The new regulations would have several major impacts on businesses in California:

- **Audit requirements:** If a business processes consumers' personal information and that processing "presents significant risk to consumers' security," it will be required to conduct a yearly cybersecurity audit.[19]

- **Risk assessments:** Most businesses subject to the CCPA would have to undertake annual risk assessments for several kinds of data use, including selling personal information, processing sensitive personal information, training automated models, and using automated decision-making for significant decisions. Those businesses would also have to receive annual certification of those assessments from the CPPA.

- **Automated decision-making ("ADMT"):** ADMT is defined as technology that processes information to replace or substantially replace "human decisionmaking," meaning that the technology can execute decisions based on its outputs "without human involvement."[20] When using ADMT, businesses must offer consumers pre-use notice, in some cases allowing consumers to opt out of ADMT's use. Consumers are entitled to this notice only when a business uses ADMT to make a "significant decision," which is defined as one that "results in the provision or denial of financial or lending services, housing, education enrollment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services."[21] That notice must give consumers both "access" to ADMT (i.e., an explanation of how the decision was made and what it was used for) and the ability to opt out. Notably, the proposed rule has been edited to remove all references to AI.

[17] *See INFORMATION FOR DATA BROKERS,* California Privacy Protection Agency, available at https://cppa.ca.gov/data_brokers/.

[18] *See Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, automated Decisionmaking Technology (ADMT), and Insurance Companies*, California Privacy Protection Agency (Nov. 22, 2024) available at https://cppa.ca.gov/regulations/ccpa_updates.html.

[19] *See Text of Proposed Regulation*, California Privacy Protection Agency, available at https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf.

[20] *Id.*

[21] *Id.*

Other changes include updates to CCPA regulations and clarifying when insurance companies must comply with its provisions. In May 2025, the CPPA opened a limited comment period, which closed June 2, 2025, indicating a goal of finalizing the regulations this fall. Public comments on the rule, were due February 25, 2025.

State Comprehensive Privacy Laws

The number of state comprehensive privacy laws grew significantly again in 2024, and we expect that trend to continue in 2025.

The newly passed and implemented laws broadly followed the pattern set by previously enacted state statutes in other states. While none of the laws included a private right of action (other than California's law that has been in effect since January 1, 2020), they grant consumers the right to (i) access their personal data and know when it is being processed; (ii) opt out of controllers selling or processing their data for targeted advertising or using it in ADMT; (iii) receive copies of their data; (iv) correct inaccurate data; (v) delete their data; (vi) be free of discrimination for exercising their rights; and (vii) appeal the denial of any of those rights. The laws also imposed common requirements on businesses, including providing notice to consumers about data practices and policies, mandating risk assessments before doing some kinds of data processing, and setting limits on the purposes for which data can be processed.

The crop of 2024 laws also introduced some novel provisions that practitioners should note:

- Rather than allowing consumers to consent to processing of their personal data in general, Maryland prohibited processing that data unless it is "strictly necessary" for a product or service the consumer requested.

- While comprehensive privacy laws typically give consumers the right to opt out of their data being processed for some kinds of profiling, Minnesota now gives consumers the right to question decisions made as a result of that profiling.

- Rhode Island allows consumers to see not only the third parties that have received their data, but also any third parties to which their data may be sold.

Privacy-law expansion will likely continue through 2025. As of July 31, 2025, comprehensive privacy laws have taken effect in two new states: Minnesota and Nebraska. Four other states will follow shortly—Indiana, Kentucky, Maryland, and Rhode Island's comprehensive privacy laws will take effect later in 2025 or January 2026. Both Colorado and Virginia passed amendments to their existing cybersecurity laws with a focus on protecting data of and advertising to minors.[22]

[22] B. Sanchez & D. Hales, *Little Users, Big Protections: Colorado and Virginia Pass Laws Focused on Kids Privacy,* Future of Privacy Forum (May 20, 2025) available at https://fpf.org/blog/little-users-big-protections-colorado-and-virginia-pass-laws-focused-on-kids-privacy/.

Meanwhile, comprehensive and sector-specific privacy bills have advanced to committees in five state legislatures (Massachusetts, Michigan, North Carolina, Pennsylvania, and Wisconsin), and numerous bills are pending in other states as well. Now that 19 states already have comprehensive privacy laws, and several are scheduled to follow suit, industry groups expect that the number of laws will keep rising, and that states will continue to write new and unique provisions into their statutes as the privacy landscape evolves.

Thus far, the growth of privacy law at the state level has not been matched by federal action. In April 2024, a bipartisan group in Congress proposed the American Privacy Rights Act—what would have been the first comprehensive federal privacy law—but the bill lost support after it was heavily modified and, later that year, died in committee. Though the prospects for such a law seem remote in the remainder of 2025, there are some signs of congressional action. The House Energy and Commerce Committee's Republican majority recently formed a data-privacy working group that hopes to develop a "framework for legislation that can get across the finish line."

Online Child Privacy Laws and First Amendment Challenges

Children's privacy continues to be a focus of legislative and regulatory efforts for both federal and state governments.

In January 2025, the Federal Trade Commission finalized changes to the Children's Online Privacy Protection Act (COPPA) to set new requirements around the collection, use, and disclosure of children's personal information. These changes offer parents new tools and protections to help them control what data about their children is provided to third parties.[23] Changes include (1) requiring opt-in parental consent for targeted advertising and other disclosures of children's personal information to third parties; (2) limiting data retention; (3) increasing Safe Harbor programs' transparency by requiring the Safe Harbor programs to publicly disclose their membership lists and report additional information; and (4) adding options for verifiable parental consent when children's personal information is not disclosed, such as a "text plus" option.

California, which has historically led the charge on privacy protections in the US, has experienced its own challenges in connection with regulating children's privacy in connection with the California Age-Appropriate Design Code Act ("CAADCA").[24] Passed in 2022, the CAADCA aims to promote strong online privacy protections for children under 18—five years older than the age covered by COPPA—and ensure that online products likely to be accessed by children "are designed in a manner that recognizes the distinct needs of children."[25] The CAADCA requires businesses providing online services likely to be accessed by children under 18 to conduct data impact protection assessments,

[23] *See* Federal Trade Commission, Children's Online Privacy Protection Rule, Final Rule Amendments, 16 CFR part 312, available at https://www.ftc.gov/system/files/ftc_gov/pdf/coppa_sbp_1.16_0.pdf.

[24] *See* 2022 Cal. Legis. Serv. Ch. 320 (A.B. 2273), available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273.

[25] *See id*; Cal. Civ. Code § 1798.99.30(b)(1).

estimate the age of users, provide default privacy settings that offer a higher level of protection for children, use language appropriate for children in privacy notices, provide transparency on tracking, and not use children's personal information for certain activities deemed harmful, such as selling personal information or tracking a child's precise geolocation.

Following enactment of the CAADCA, the US District Court for the Northern District of California granted a national trade association's request for a preliminary injunction challenging the law's constitutionality. An August 2024 Ninth Circuit opinion partially affirmed and partially vacated this preliminary injunction.[26] The Ninth Circuit found that the plaintiff was likely to succeed in showing that the CAADCA violates the First Amendment by requiring businesses to form an opinion on and mitigate the risk of children's exposure to (potentially) harmful materials. The court, therefore, affirmed the injunction as to the enforcement of that requirement.[27] But the court vacated the remainder of the injunction because the record did not clearly show whether the CAADCA's other provisions facially violate the First Amendment.[28] The case was remanded to the District Court and litigation is ongoing.

In 2025, we expect that we may see further challenges to privacy law requirements based on First Amendment arguments.

Meanwhile, other states are also seeking to add privacy protections for children under 18. For instance, New York's Child Data Protection Act was signed into law in 2024 and took effect June 20, 2025. This act aims to protect minors from having their personal data accessed.

California Invasion of Privacy Act Litigation

Plaintiffs-side litigators have been testing novel applications of the 1967 California Invasion of Privacy Act (CIPA) to websites generating mixed results and, therefore, creating a conflicting web of judicial authorities. CIPA prohibits wiretapping without consent and prohibits the use of "pen registers" or "trap and trace" devices, technology historically used to capture incoming and outgoing phone numbers on telephones.[29] CIPA imposes potential penalties of US$5,000 per violation, plus attorneys' fees. Plaintiffs are increasingly seeking to stretch CIPA's prohibitions on "pen registers" and "trap and trace devices" to internet websites for third-party IP collection tools.

Federal and state courts in California have split on whether CIPA's definitions for pen registers would apply to website tools that collect information, such as IP addresses, from visiting users.[30]

---

[26] *See Netchoice, LLC v. Bonta*, No. 23-2969, (9th Cir. Aug. 16, 2024) available at https://cdn.ca9.uscourts.gov/datastore/opinions/2024/08/16/23-2969.pdf.

[27] *Id.*

[28] *Id.*

[29] Cal. Pen. Code § 638.51.

[30] *Compare Shah v. Fandom, Inc.*, 754 F. Supp. 3d 924 (N.D. Cal. 2024) (holding that CIPA definition was ambiguous but that website tracking qualified) *with Sanchez v. Cars.com Inc., 2025 WL 487194 (Cal. Super. Jan. 27, 2025)* (holding that CIPA only applied to "mechanical, telephone number-tracing technology, not technology used to collect the IP address from a desktop computer").

Courts have also gone both ways on the question of whether third-party technology embedded on websites constitutes a third-party interception (which requires consent) or a party to the communication (which does not).[31] Courts continue to evaluate CIPA claims for internet tracking on a case-by-case basis, and on Friday, August 1, a jury in the Northern District of California exemplified the risks facing businesses by finding that Meta violated a class of plaintiffs' rights under CIPA by collecting data from a fertility tracking app, Flo Health.[32] On the same day, a California state court issued a significant ruling in *Heiting vs. HP Inc*., dismissing a CIPA claim that alleged HP's use of third-party website tracking software constituted an illegal "trap and trace" device. The court held that the website tools in question did not fall within the CIPA's statutory definition of a trap and trace device, emphasizing that the statute targets devices capturing unauthorized information about incoming communications from third parties, not information exchanged directly between a website and its user and noting that to read otherwise would "[go] far afield from any concept of wiretapping . . . . there is no indication that, in enacting the trap and trace device prohibition, the California Legislature meant to cover such devices."[33]

In May 2025, California legislators introduced a bill amending CIPA to allow for tracking for "commercial business purposes," in theory to limit future cookie-related litigation.[34] While the bill passed unanimously in the California Senate in June, the California Assembly designated it a "two-year bill" to allowing for continued study of the issue and guaranteeing that no action will be taken until 2026, at the earliest. Businesses, therefore, should ensure that their cookie banners use clear language, are easy to read, and present consumers with equal, symmetrical choices and should continue to monitor developments in this area for the remainder of 2025, and into 2026, until either the California legislature acts to clarify the scope and application of CIPA or judicial authorities coalesce on consistent interpretation.

Consent

Courts continue to recognize the enforceability of clickwrap, sign-in wrap, and browsewrap consent agreements, but they distinguish the burden that each method of privacy notice and disclosure places on the company. Clickwrap agreements require an affirmative confirmation of the privacy disclosure by the visitor of a website. As the Ninth Circuit concluded last year, these agreements are generally enforceable. *See Wynn v. United Parcel Serv., Inc.,* No. 23-15448, 2024 WL 1191143, at *1 (9th Cir. Mar. 20, 2024) (finding no violation of a statute requiring clear, conspicuous, and stand-

[31] *Compare In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020) (holding Facebook was not exempt from liability as a matter of law under CIPA as a party to the communication where plaintiffs alleged the social media platform had caused simultaneous unknown duplication and transmission of plaintiffs' communications with third-party sites) *with In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 152 (3d Cir. 2015) (holding that Google was a party to the electronic transmissions that were the bases for the plaintiffs' wiretapping claims and that such claims must be dismissed).

[32] Kat Black, *This Verdict is a Wake-Up Call: Jury Trial Finds Meta Breached State Privacy Law in Class Action Against Fertility App*, Law.com (Aug. 1, 2025) available at https://www.law.com/therecorder/2025/08/01/this-verdict-is-a-wake-up-call-jury-trial-finds-meta-breached-state-privacy-law-in-class-action-against-fertility-app-/.

[33] *Heiting vs. HP Inc.,* No. 24STCV29634, 4-5 (Cal. Super. Ct. of Los Angeles 2025).

[34] V. Smolczynski & K. McConnell, *California Senate Bill Seeks to Curb Cookie-Related CIPA Litigation,* Carpe Datum Law (May 16, 2025) available at https://www.carpedatumlaw.com/2025/05/california-senate-bill-seeks-to-curb-cookie-related-cipa-litigation/.

alone disclosure where the company included a checkbox below the disclosure); *see also Berman v. Freedom Fin. Network, LLC*, 30 F.4th 849, 856 (9th Cir. 2022) (finding clickwrap agreements enforceable).

Browsewrap agreements, such as those premised solely on the posting of terms of use and a privacy policy linked on the home page of a website (even if the posting is required by the CCPA), may fall on the other end of the spectrum. Instead of an affirmative confirmation of the privacy disclosure, the case for consent is premised on constructive notice and an inference that privacy disclosures have been reviewed by users that continue to use the website. Browsewrap agreements also can be enforceable in some circumstances, but courts often require some basis to conclude that the visitor was aware of the terms of its policy. If the company can show that the website "puts a reasonably prudent user on inquiry notice of the terms of the contract," the browsewrap agreement is enforceable. *See, e.g. Nguyen v. Barnes & Noble, Inc.*, 763 F.3d 1171, 1176-77 (9th Cir. 2014). Within the Ninth Circuit, courts have found constructive assent by evaluating "the conspicuousness and placement of the 'Terms of Use' hyperlink, other notices given to users of the terms of use, and the website's general design" in determining "whether a reasonably prudent user would have inquiry notice" of such terms. *Allen v. Shutterfly*, *Inc.*, No. 20-cv-02448, 2020 WL 5517172, at *6 (N.D. Cal. Sept. 14, 2020). At least on the pleading stage, dismissal arguments based on browsewrap agreements have had mixed results.

Sign-wrap agreements fall between clickwrap and browsewrap. Visitors are not asked to specifically accept the privacy policy, but the privacy policy is connected to another action, such as the act of completing a purchase on the website. These agreements are enforced when there is some affirmative action indicating consent. *See, e.g. Silver v. Stripe Inc.*, No. 4:20-cv-08196, 2021 WL 3191752, at *3 (N.D. Cal. July 28, 2021) (finding consent in the context of an Instacart sign-wrap agreement when an order is placed).

Recommendations for Cookie Collection

Considering the uptick in litigation over cookie-collection practices, businesses are strongly advised to use cookie banners on their websites. This risk mitigation may be most significant for California visitors, and some companies have geo-fenced California or otherwise treated California differently. Cookie banners may allow companies to comply with the notice-at-collection requirement under the CCPA and to avoid wiretap and invasion-of-privacy claims. It is advisable for businesses to set up their website such that it sends only strictly necessary cookies to the visitor's device before obtaining consent, does not utilize pre-ticked boxes for cookies settings, and includes a link to the privacy policy and cookie policy on the banner. Users should be permitted to manage their cookie settings through this cookie banner, allowing them to decide which cookies they want to remain active.

Federal Enforcement and Regulations: Heightened Scrutiny and Costly Lapses

Public companies should expect continued federal scrutiny of their cybersecurity procedures in 2025. The SEC's efforts to amend Regulation S-P and issue guidance on cybersecurity requirements suggest the search for a balance between over-sharing and under-reporting remains ongoing. But the Department of Justice has been clearer in its enforcement priorities, using the False Claims Act against federal contractors to underscore the risk of ignoring cybersecurity requirements.

Evolving SEC Requirements

- In April 2025, Paul S. Atkins was sworn in as SEC chairman. Atkins has indicated that, under his leadership, SEC priorities will include protecting investors from fraud through "smart," "effective," and "appropriately tailored" regulation designed to promote innovation and not stifle business.[35] While some stakeholders await an anticipated shift towards de-regulation in the coming months of the Trump administration as a general matter, the SEC has noted that it will continue to enforce certain cybersecurity standards, such as Regulation S-P, although its interpretation of materiality may be a higher bar than previously indicated.[36] Members of current SEC leadership have articulated in the past a view that the Cybersecurity Rules are overbearing and burdensome, dissenting from enforcement actions in October of 2024.[37] In their dissent from enforcement against several SolarWinds customers in 2024, Commissioners Hester M. Peirce and Mark T. Uyeda indicated that the SEC's view of materiality was overbroad and potentially leading to immaterial disclosure.[38] For example, Peirce and Uyeda criticized the Commission's judgment of materiality in the SolarWinds case as the Commission "donning a Monday morning quarterback's jersey to insist that immaterial information be disclosed" in a way that does the "opposite" of protecting investors.[39] In recent remarks before the Senate, Chairman Paul S. Atkins further made reference to the need for more tailored disclosure requirements, stating that, under his leadership, the SEC will make sure that investors get disclosures that "actually help them" understand investment risks.[40] These statements, paired with a current rise in calls for the SEC to rescind the rules

[35] *See* Paul S. Akins, Chairman, *Testimony Before the United States House Appropriations Subcommittee on Financial Services and General Government*, United States Security & Exchange Commission (May 20, 2025) https://www.sec.gov/newsroom/speeches-statements/atkins-testimony-fsgg-052025.

[36] *See* Keith Cassidy, Acting Director, Division of Examinations, *Regulation S-P – Back to the Future*, United States Security & Exchange Commission (May 14, 2025) https://www.sec.gov/newsroom/speeches-statements/cassidy-remarks-finra-conference-051425.

[37] See H. M. Peirce, Commissioner, and Mark T. Uyeda, Commissioner, *Statement Regarding Administrative Proceedings Against SolarWinds Customers*, United States Security & Exchange Commission (Oct. 22, 2024) https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-solarwinds-102224.

[38] *Id.*

[39] *Id.*

[40] *See* Paul S. Atkins, Chairman, *Testimony Before the United States Senate Appropriations Subcommittee on Financial Services and General Government*, United States Security & Exchange Commission (June 3, 2025) https://www.sec.gov/newsroom/speeches-statements/testimony-atkins-060325.

from prominent business groups, could impact the trajectory of SEC cybersecurity regulation during the remainder of 2025 and beyond.[41]

- Various industry groups have viewed the change in administration as an opportunity for change, specifically to rescind the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule. On May 22, 2025, several financial trade associations petitioned the SEC to rescind the cybersecurity regulation due to the rule allegedly resulting in "premature disclosure" and "significant confusion" that has "harmed registrants and failed to provide the market with meaningful or actionable information upon which to make investment decisions."[42] In their letter, the trade organizations, which include the American Bankers Association, the Bank Policy Institute, the Securities Industry and Financial Markets Association, the Independent Community Bankers of America, and the Institute of International Bankers, urged the SEC to rescind the reporting requirements under Form 8-K Item 1.05 and Form 6-K and instead develop a "balanced cyber disclosure regime" that follows the SEC's "investor protection mandate."[43]

- In addition to the disclosure requirements discussed above, companies should continue to monitor the impact of the SEC's August 2024 amendments to Regulation S-P, which require broker-dealers, investment companies, registered investment advisors, funding portals, and registered transfer agents to take additional steps with respect to documenting incident response procedures and other efforts to address unauthorized access to or use of customer information. Speaking at a FINRA conference on May 14, 2025, Acting Director of the Division of Examinations Keith Cassidy highlighted the "importance of, and the financial sector's role in, information security and the protection of investors' nonpublic personal information." Cassidy indicated that the Division of Examinations would host a series of three "tailored outreach events" to assist firms in preparedness to implement the Regulation S-P amendments.[44] Cassidy also previewed that the Division of Examinations could communicate anonymized observations through a Risk Alert or other publication to the extent staff identifies risks relevant across a particular sector or registrant population.[45] Given this recognition of the amendments' importance to ensure security of customer information and protection against security threats, companies should prepare to comply with

[41] See H. M. Peirce, Commissioner & M.T. Uyeda, Commissioner, *Statement Regarding Administrative Proceedings Against SolarWinds Customers*, United States Security & Exchange Commission (Oct. 22, 2024) https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-solarwinds-102224.

[42] *See Petition for Rulemaking on the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule* (May 22, 2025) www.sifma.org/wp-content/uploads/2025/05/Joint-Financial-Trades-Final-Petition-for-Rulemaking-on-Cybersecurity-Risk-Management-Strategy-Governance-and-Incident-Disclosure-Rule.pdf.

[43] *Id.*

[44] See Keith Cassidy, Acting Director, Division of Examinations, *Regulation S-P – Back to the Future* (May 14, 2025) https://www.sec.gov/newsroom/speeches-statements/cassidy-remarks-finra-conference-051425.

[45] *Id.*

the Regulation S-P amendments and monitor additional guidance from the SEC as examinations commence.

- Internal reorganizations at the SEC may reflect a change in enforcement priorities as well. In February 2025, the SEC announced the replacement of the Crypto Assets and Cyber Unit with the Cyber and Emerging Technologies Unit (CETU), consisting of approximately 30 fraud specialists and attorneys with instructions to deploy enforcement resources "judiciously" in the pursuit of investor protection.[46] Mark T. Uyeda, Acting Chairman at the time of CETU's announcement, praised the unit for "protect[ing] investors" as well as facilitating capital formation and market efficiency by "root[ing] out those seeking to misuse innovation" to "diminish confidence in new technologies."[47] The CETU's focuses will purportedly include "combatting cyber-related misconduct" particularly in the emerging technologies space, including enforcing regulated entities' compliance with cybersecurity regulations and investigating fraud committed using emerging technologies like machine learning and AI.[48] Companies involved in the artificial intelligence, machine learning, and other emerging technology industries should continue to monitor guidance from this unit and enforcement actions to the extent any arise during the remainder of 2025.

Heightened DOJ Enforcement Against Federal Contractors

The Department of Justice's Civil Cyber-Fraud Initiative, announced in 2021, continues to push companies to comply with federal cybersecurity standards. By using the False Claims Act (FCA) to punish federal contractors for allegedly failing to comply with federal cybersecurity requirements, the DOJ has recovered nearly US$30 million in just four years. 2024 saw new milestones in the federal government's use of the FCA to ensure the protection of federal data and recoveries through 2025 indicate that settlement amounts will continue to rise.

FCA Background

Under the FCA, any entity that does business, directly or indirectly, with the government can be held liable for submitting or causing the submission of a false or fraudulent claim for payment.[49] If found liable, a defendant faces civil penalties for each claim for payment, actual damages valued at the amount the government paid toward the claims, and treble the amount of actual damages.[50]

[46] See *SEC Announces Cyber and Emerging Technologies Unit to Protect Retail Investors*, United States Security & Exchange Commission (Feb. 20, 2025) https://www.sec.gov/newsroom/press-releases/2025-42.
[47] *Id.*
[48] *Id.*
[49] 31 U.S.C § 3729
[50] 31 U.S.C § 3730

Key to the FCA is its *qui tam* provision, which allows private whistleblowers (also known as relators) to pursue claims on behalf of the government and receive up to 30% of any recovery.[51] Relators' suits are filed under seal and kept secret while the DOJ decides whether to intervene and litigate the case or allow the relator to pursue the case independently.[52] The *qui tam* provision provides a powerful incentive for anyone with knowledge of a contractor's policies and procedures to report alleged misconduct.

Many federal contracts include express certifications that the contractor will comply with federal requirements, including statutes, rules, and contractual clauses, and FCA suits often concern whether a defendant's certification of compliance with these requirements was knowingly false. But the FCA also covers "implied false certifications," where a company faces liability for failing to disclose noncompliance with federal requirements even where it did not expressly certify compliance.

The Rise in Cyber-Fraud Recoveries

Relators have targeted companies' compliance with National Institute of Standards and Technology (NIST) provisions as a basis for FCA litigation. These standards are frequently written into federal contracts and require contractors to provide "adequate" security for access to government data and information. Adequate is defined as, at minimum, compliance with the NIST Special Publication 800-171, titled "Protecting Uncontrolled Unclassified Information in Nonfederal Information Systems and Organizations." NIST 800-171 includes over 100 security requirements covering topics including access control, incident response, personnel security, and system and information integrity.

O'Melveny previously predicted that the Civil Cyber-Fraud Initiative would seize on NIST standards because their ambiguity and vagueness would provide the DOJ and regulators the opportunity to assert that a contractor has misinterpreted the standards and, therefore, falsely certified compliance. Ambiguity includes NIST 800-171 section 3.11.2, which states that a company should scan for vulnerabilities in its organizational systems and applications "periodically" without any explicit instructions on how organizations should conduct these scans or what "periodically" means. The prediction came to bear in 2024 when the DOJ intervened in its first Cyber-Fraud Initiative case—alleging that the Georgia Institute of Technology and Georgia Tech Research Corp. failed to meet NIST standards under their Department of Defense contracts.[53]

Last year was also a banner year for Cyber-Fraud Initiative recoveries, which came from a trio of companies that allegedly failed to adequately protect data collected as part of Covid-19 programs

[51] *Id.*

[52] *Id.*

[53] United States' Complaint-In-Intervention, *United States ex rel. Craig v. Ga. Tech Rsch. Corp.*, 1:22-cv-02698-JPB, Dkt. 23 (N.D. Ga. Aug. 22, 2024).

funded by federal grants.[54] Guidehouse Inc. and housing organization Nan McKay received a contract from New York State to create a website for residents to apply for federal rental assistance during the pandemic, paid for in part with federal grant funding. Shortly after the website went live, the companies determined that the personally identifiable information they were collecting was viewable using commercial search engines and shut the website down. Both companies settled with the DOJ for a combined US$11.3 million and admitted that they did not conduct the required testing to ensure that the website was secure.[55]

Insight Global LLC received a contract from the Pennsylvania Department of Health—funded, in part, through a grant from the US Centers for Disease Control and Prevention—to conduct contact tracing during the pandemic. Insight allegedly transferred personally identifiable information in the body of unencrypted emails and stored the data in unencrypted Google files that were not password protected and were accessible to the public via internet links. After a breach involving data from 72,000 individuals, Insight settled a private suit for up to US$250 per impacted individual[56] and paid US$2.7 million to resolve FCA allegations that the company failed to follow federal standards for data protection.[57]

The Cyber-Fraud Unit's actions so far this year indicate that the trend in larger recoveries will continue. On February 28, 2025, the Department of Justice announced that Health Net Federal Services Inc. and its corporate parent, Centene Corporation, agreed to pay US$11,253,400 to resolve claims that Health Net falsely certified compliance with cybersecurity requirements in its contract with the Department of Defense to administer a health benefits program for service members. Centene acquired Health Net in 2016 and, notably, the settlement resolved allegations concerning noncompliance with cybersecurity obligations from 2015-2018. On March 26, 2025, The Department announced a US$4,600,000 settlement for a defense contractor's alleged failure to comply with Department of Defense cybersecurity requirements for use of a third-party email system.[58] On May 1, 2025, The Department announced a US$8,400,000 settlement with Raytheon and Nightwing Group (which had acquired the relevant Ratheon subsidiary in 2024) for allegedly failing to store covered defense information and federal contact information relating to 29 government contracts between 2015 and 2024.[59] And, on July 30, 2025, DOJ announced a US$9,800,000 settlement with Illumina Inc. to resolve whistleblower allegations that Illumina Inc.,

[54] Office of Public Affairs, *False Claims Act Settlements and Judgments Exceed $2.9B in Fiscal Year 2024*, DOJ (Jan. 15, 2025) available at https://www.justice.gov/archives/opa/pr/false-claims-act-settlements-and-judgments-exceed-29b-fiscal-year-2024

[55] Office of Public Affairs, *Consulting Companies to Pay $11.3M for Failing to Comply with Cybersecurity Requirements in Federally Funded Contract*, DOJ (June 17, 2024) available at https://www.justice.gov/archives/opa/pr/consulting-companies-pay-113m-failing-comply-cybersecurity-requirements-federally-funded.

[56] Steve Alder, Insight Global Settles Class Action Data Breach Lawsuit, The HIPPA Journal (Apr. 13, 2023) available at https://www.hipaajournal.com/insight-global-settles-class-action-data-breach-lawsuit/.

[57] Office of Public Affairs, *Staffing Company to Pay $2.7M for Alleged Failure to Provide Adequate Cybersecurity for COVID-19 Contact Tracing Data*, DOJ (May 1, 2024) available at https://www.justice.gov/archives/opa/pr/staffing-company-pay-27m-alleged-failure-provide-adequate-cybersecurity-covid-19-contact.

[58] Parker Quinlan, Defense Contractor to Pay $4.6M Over Cyber Compliance, LAW360 (March 26, 2025) available at https://www.law360.com/articles/2316054/defense-contractor-to-pay-4-6m-over-cyber-compliance.

[59] MJ Koo, Raytheon, Nightwing to Pay Feds $8.4 M Over Cybersecurity, LAW360 (May 1, 2025) available at https://www.law360.com/articles/2333118/raytheon-nightwing-to-pay-feds-8-4m-over-cybersecurity.

"failed to incorporate product cybersecurity into its software design, development, installation and marketing," "failed to properly support personnel and systems tasked with product security," and "failed to correct design flats that created cybersecurity vulnerabilities" in gene sequencing devices sold to federal government agencies.[60]

Ramifications for Federal Contractors

The DOJ's leverage of the FCA in the cybersecurity space underscores the importance of understanding any cybersecurity obligations that a company or contractor has to protect government data pursuant to a government contract. The DOJ's intervention in Georgia Tech's case and the growing size of recoveries indicate that cybersecurity compliance will be a continued focus for the government. Companies should be sure to scrutinize any cybersecurity obligations contained in government contracts and consider:

- auditing cybersecurity components to ensure compliance with the NIST standards and plan to conduct routine assessments of security protocol sufficiency;
- whether any contract between the company and a state or municipality or between the company and another private party is federally funded and potentially includes cybersecurity requirements;
- whether a potential data breach indicates noncompliance with cybersecurity requirements maintained in federal contracts; and
- when approaching the potential acquisition of another entity, auditing the data it retained pursuant to any federal contracts and its cybersecurity protocols.

US Data Security Program to Address National Security Risks

In February 2024, President Biden issued Executive Order 14117, directing the DOJ to issue regulations for preventing access to sensitive personal and government-related data by "Countries of Concern or Covered Persons"—a category that encompasses certain entities or persons in China, Hong Kong, Macau, Russia, Iran, North Korea, and Venezuela. On January 8, 2025, the DOJ issued a final rule (the "Data Security Program") implementing those restrictions and protections, that generally prohibits the transfer of "bulk sensitive personal data" to such countries without a license from the US government.[61]

[60] Office of Public Affairs, *Illumina Inc. to Pay $9.8M to Resolve False Claims Act Allegations Arising from Cybersecurity Vulnerabilities in Genomic Sequencing Systems,* DOJ (July 31, 2025) available at https://www.justice.gov/opa/pr/illumina-inc-pay-98m-resolve-false-claims-act-allegations-arising-cybersecurity.

[61] *See 28 C.F.R. Part 202.*

This includes certain types of personal identifiers, precise geolocation data, biometric identifiers, human "omic" data, personal health data, and personal financial data. Companies that have operations or do business in, or with touchpoints to, China, Hong Kong, or Macau should review these requirements to determine if they apply and what steps they need to take to comply with these new cross-border restrictions. US entities and individuals are required to comply with the Data Security Program's prohibitions and restrictions, and with all other provisions of the Data Security Program with the exception of the affirmative obligations of subpart J (related to due diligence and audit requirements for restricted transactions), § 202.1103 (related to reporting requirements for certain restricted transactions), and § 202.1104 (related to reports on rejected prohibited transactions), which become effective October 6, 2025. The Department of Justice has issued guidance (Guidance)[62] to assist individuals and entities in complying with the Data Security Program. The Guidance includes a Compliance Guide, FAQs, and an Implementation and Enforcement Policy.

International Developments in Cybersecurity Law

On the international front, US companies should be aware of several key developments:

New India Data Protection Laws

In January 2025, India released a draft of proposed rules under the recently passed the Digital Personal Data Protection Act (DPDP Act), the nation's first comprehensive data privacy legislation regulating digital personal data processing. The proposed rules were open for public comment through mid-March and while not yet in effect, provide a preview of the likely number of significant new data privacy and security obligations that will come into effect for those processing digital personal data within India—and outside of the country if such processing relates to goods or services offered to individuals within India. Companies with operations in or doing business in India should continue to monitor for publication of these rules once finalized so that they are in a position to comply when they take effect. The current expected regulatory framework includes:

- **Consent:** Explicit written consent is required for the collection of an individual's sensitive personal data or information.
- **Data Breach Notice:** Similar to the European Union's General Data Protection Regulation (GDPR), the data controller is required to give notice to India's enforcement authority (the Data Protection Board) and to affected data subjects within 72 hours from discovery of a data breach.

[62] *See Data Security Program: Compliance Guide,* Department of Justice (Apr. 11, 2025) available at https://www.justice.gov/opa/media/1396356/dl.

- **Security Measures:** The proposed rules describe detailed security measures and safeguards that must be adopted to protect personal data and prevent security breaches. In addition, security provisions must be included in contracts between data controllers and data processors.

- **Data Protection Officer:** In certain cases, the data controller must appoint a data protection officer based in India.

- **Children and Persons with Disabilities:** The data controller must obtain verifiable parental consent before collecting personal data of children or persons with disabilities. Under the DPDP Act, children are defined as any person under the age of 18, which is older than the applicable definitions under the GDPR and US law.

- **Deletion Requirements:** E-commerce platforms with over 20 million registered users, online gaming intermediaries with over 5 million users, and social media intermediaries with over 20 million users must delete user data after three years of inactivity.

- **Cross-Border Transfers:** The DPDP Act authorizes the Data Protection Board to issue regulations governing cross-border transfers to certain restricted/prohibited territories. Such territories and the conditions for cross-border transfers have not yet been identified.

- **Annual Data Protection Impact Assessments (DPIAs):** If the Indian government identifies an entity as a "significant data fiduciary" based on such factors as volume and sensitivity of the data processing, that entity must conduct annual DPIAs to assess risks associated with its data processing activities and submit its findings to the Data Protection Board.

Amendments to Australia Privacy Act

In December 2024, Australia amended its Privacy Act to make a number of significant changes that will take effect over the next year or so. These include creating a private right of action for invasion of privacy and imposing transparency obligations to disclose when decisions are made using automated processes. New measures have also been introduced to:

- combat doxing, making it illegal to share someone's personal information with the intent to harm;

- develop a privacy code addressing online privacy for children, giving the data protection agency the power to "whitelist" countries that provide substantially similar privacy protections;

- issue infringement notices and compliance notices; and
- require that "reasonable steps" be taken to protect the security of personal information, including implementing technical and organizational measures.

Companies with operations in or doing business in Australia should review and begin preparing to comply with these requirements.

Conclusion

We saw heightened legislative and regulatory activity in 2024 and early 2025 to address rapidly emerging cybersecurity and data privacy issues. Those trends will likely intensify for the rest of this year as developments in AI technology and increased consumer awareness of privacy issues spark increased consumer protection efforts. Companies will need to stay alert to their evolving obligations.

KEY CONTACTS

Randall W. Edwards
Partner
San Francisco
+1 415 984 8716
redwards@omm.com

Sid Mody
Partner
Dallas
+1 945 221 1645
smody@omm.com

Amanda M. Santella
Partner
Washington, DC
+1 202 383 5403
asantella@omm.com

Reema Shah
Partner
New York
+1 212 728 5710
rshah@omm.com

David J. Ribner
Partner
Washington, DC
+1 202 383 5507
dribner@omm.com

Scott W. Pink
Special Counsel
Silicon Valley
+1 650 473 2629
spink@omm.com

Hannah E. Dunham
Counsel
Los Angeles
+1 213 430 8162
hdunham@omm.com

Becky Girolamo
Counsel
Los Angeles
+1 213 430 6240
bgirolamo@omm.com

Sabrina E. van der Linden-Gonzales
Counsel
Newport Beach
+1 949 823 7157
svanderlinden-gonzales@omm.com

Joshua Goode
Associate
Washington, DC
+1 202 383 5332
jgoode@omm.com

Andrew Kus
Associate
San Francisco
+1 415 984 8741
akus@omm.com

Emily Losi
Associate
New York
+1 212 728 5931
elosi@omm.com

Vy N. Malette
Associate
Newport Beach
+1 949 823 6989
vnguyen@omm.com

Max J. Rosenthal
Associate
Washington, DC
+1 202 383 5250
mrosenthal@omm.com

This white paper is a summary for general information and discussion only and may be considered an advertisement for certain purposes. It is not a full analysis of the matters presented, may not be relied upon as legal advice, and does not purport to represent the views of our clients or the Firm. Randall W. Edwards, an O'Melveny partner licensed to practice law in California; Sid Mody, an O'Melveny partner licensed to practice law in Texas; Amanda M. Santella, an O'Melveny partner licensed to practice law in the District of Columbia and Maryland; Reema Shah, an O'Melveny partner licensed to practice law in New York; David J. Ribner, an O'Melveny partner licensed to practice law in the District of Columbia and New York; Scott W. Pink, an O'Melveny special counsel licensed to practice law in California; Hannah E. Dunham, an O'Melveny counsel licensed to practice law in California and the District of Columbia; Becky Girolamo, an O'Melveny counsel licensed to practice law in California; Sabrina E. van der Linden-Gonzales, an O'Melveny counsel licensed to practice law in California; Joshua Goode, an O'Melveny associate licensed to practice law in the District of Columbia; Andrew Kus, an O'Melveny associate licensed to practice law in California; Emily Losi, an O'Melveny associate licensed to practice law in New York; Vy N. Malette, an O'Melveny associate licensed to practice law in California; Max J. Rosenthal, an O'Melveny associate licensed to practice law in the District of Columbia; and Vivienne Reed, an O'Melveny law clerk, contributed to the content of this white paper. The views expressed in this white paper are the views of the authors except as otherwise noted.