Coblentz
Patch Duffy
& Bass LLP

2024 Mid-Year Privacy Report

A Comprehensive Look at New Developments in Data Privacy Laws

Coblentz Patch Duffy & Bass LLP
One Montgomery Street, Suite 3000
San Francisco, CA 94104

coblentzlaw.com

Summer 2024

Contents

Introduction

2024 has been another big year for privacy. Several new state privacy laws are going into effect, with several more coming in 2025, while a federal privacy law continues to be discussed that would further change the privacy landscape across the country. Meanwhile, hot topics like artificial intelligence ("AI"), minors' privacy rights, and international data flows continue to be at the forefront of proposed and recently enacted legislation and regulations. Seeing how all of these new laws and regulations are being enforced and will continue to be enforced by regulators is still in the very early stages. And privacy litigation has seen an uptick due to novel legal theories around the use of website tracking technologies. There are certainly many issues for companies to put on their privacy "To Do List" for the remaining months of 2024.

New State Privacy Laws

In 2023, companies were focused on compliance with new state privacy laws in Colorado, Connecticut, Utah, and Virginia, as well as California's CPRA amendments to the CCPA. 2024 sees four more state privacy laws going into effect in Florida, Montana, Oregon, and Texas, with eight new state privacy laws just around the corner in 2025.[1] As we are now past the mid-point of the year, companies should be assessing their compliance with the newly effective state laws and planning for those going into effect next year.

General Principles of State Privacy Laws

For the most part, companies can at least find some comfort in the fact that the new laws coming into effect focus on many of the same general principles as the privacy laws already in effect, including requirements to provide clear notices to consumers about how data is collected, used, and disclosed, as well as imposing purpose and use limitations on the data collected. This means that businesses should ensure they are only collecting data that they actually need for legitimate business purposes and using it only for the purposes being disclosed in clear and conspicuous privacy notices. Additionally, consumer privacy rights are generally consistent across the state laws, including rights of access, appeal[2], portability, correction[3], and deletion, as well as the right to opt-out of sales and sharing of information for targeted advertising purposes.

Differences in State Privacy Laws

However, there are some nuances that may pose some problems for businesses as they seek to develop consistent privacy practices across all U.S. states. These nuances include the fact that many—but not all—recently enacted privacy laws have moved away from an opt-out regime, e.g., California, and towards an opt-in regime for the collection and use of "sensitive" personal data, which typically includes Social Security numbers, biometric data, health data, financial data, and data about protected characteristics, among other categories. Perhaps most importantly for businesses engaged in targeted advertising, precise geolocation (e.g., geolocation within about 1750-1850 feet, such as through GPS tracking) falls within the definition of "sensitive" data under many new state laws. If companies are collecting that information, they are required under several state laws to obtain affirmative opt-in consent before collecting and processing that information. Moreover, some state laws also require that companies provide consumers with an option to opt-out of profiling and certain automated decision-making processes, including those involving artificial intelligence. And many new state laws require that companies conduct data protection impact assessments ("DPIAs") and/or internal or external audits if they engage in "high risk" processing,

1 Laws going into effect in 2025 include Delaware, Iowa, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, and Tennessee. Additionally, laws have already been passed in Indiana, Kentucky, and Rhode Island that are scheduled to take effect in 2026.

2 To date, the only state that does not currently have a right to appeal is California. However, we anticipate this may change as California is likely to update to be consistent with other states in this regard.

3 The only states that do not have a right to correction are Iowa and Utah.

which generally includes selling or sharing of data for targeted advertising purposes, profiling, or the processing of "sensitive" personal information.

All of these new and varied requirements mean that now, more than ever, businesses need to understand what laws apply to their collection and processing of data and what requirements exist under applicable laws. With the advent of increased concerns by consumers and citizens alike, state regulators in many states have promised aggressive enforcement of their privacy laws.

Applicability of State Privacy Laws

Determining whether any or all of the new state privacy laws apply to your business is also somewhat complicated. Most states have not followed California's approach of using annual gross revenue ($25M) as a trigger for applicability. Instead, most states have focused on volume-based triggers, with most state privacy laws applying to companies that "do business in the state" and collect the personal data of 100,000 or more residents of that state. There are outliers, however, with Montana only requiring the collection of the personal information of 50,000 residents for the law to apply and Maryland, New Hampshire, and Delaware (all going into effect in 2025) and Rhode Island (going into effect in 2026) only requiring the processing of 35,000 residents' information for the laws to apply. Texas is the primary outlier of concern for many businesses, as its privacy law applies broadly to any company doing business in Texas or producing a product or service consumed by Texas residents, as long as the company is not a "small business" as defined by the U.S. Small Business Administration. An outlier on the other end of the spectrum is Florida, as most of its requirements and restrictions apply to data controllers that conduct for-profit business in Florida and have an annual gross revenue exceeding $1 billion.

Enforcement of State Privacy Laws

In terms of enforcement, businesses can continue to breathe a sigh of relief that none of the new state laws include a private right of action for violation of their requirements. Rather, all the new state laws are enforced by state regulators, which at least has the effect of reducing plaintiff-lawyer-driven privacy litigation under state privacy laws. California remains the only state with a private right of action, but that right is limited to data breaches involving a breach of sensitive personal information. Notably, Vermont passed a privacy law in May that included a broad private right of action for violation of the law, but the law was vetoed by the governor in June.

Key Takeaways

In sum, twenty states have now passed comprehensive privacy laws, with several other states currently addressing similar privacy legislation. Although there is always talk of a federal law that might harmonize privacy requirements across the country, see *Federal Privacy Law (Again)* on page 7, that talk has been ongoing – with no federal law resulting therefrom – for many years. Companies hoping to avoid compliance with recently effective and soon-to-be effective state privacy laws should not rely on a federal privacy law to save them from compliance efforts. Now is the time to take a hard look at what laws apply to your company and take steps to ensure compliance.

State Privacy Laws Effective Dates and Applicability Thresholds

State	Effective Date	Applicability Threshold
California	January 1, 2020	$25M+ Annual Revenue OR processing data of 100,000+
Virginia	January 1, 2023	Processing data of 100,000+
Colorado	July 1, 2023	Processing data of 100,000+
Connecticut	July 1, 2023	Processing data of 100,000+
Utah	December 31, 2023	$25M+ Annual Revenue AND processing data of 100,000+
Florida	July 1, 2024	$1B+ Annual Revenue
Oregon	July 1, 2024	Processing data of 100,000+
Texas	July 1, 2024	Conducts business in Texas or produces product or service consumed by Texas residents and is not a “small business”
Montana	October 1, 2024	Processing data of 50,000+
Delaware	January 1, 2025	Processing data of 35,000+
Iowa	January 1, 2025	Processing data of 100,000+
Nebraska	January 1, 2025	Conducts business in Nebraska or produces product or service consumed by Nebraska residents and is not a “small business”
New Hampshire	January 1, 2025	Processing data of 35,000+
New Jersey	January 15, 2025	Processing data of 100,000+
Tennessee	July 1, 2025	$25M+ Annual Revenue AND processing data of 100,000+
Minnesota	July 31, 2025	Processing data of 100,000+
Maryland	October 1, 2025	Processing data of 35,000+
Indiana	January 1, 2026	Processing data of 100,000+
Kentucky	January 1, 2026	Processing data of 100,000+
Rhode Island	January 1, 2026	Processing data of 35,000+

Federal Privacy Law (Again)?

Last year, we reported on the American Data Privacy and Protection Act ("ADPPA"), a proposed federal privacy bill that ultimately failed the House or Senate. This year, another proposed federal privacy bill, the American Privacy Rights Act of 2024 ("APRA") builds on the foundation of the ADPPA. While it is still early in the legislative process, this bicameral, bipartisan draft legislation has many wondering if this could finally be the legislation that creates a federal privacy law.

The APRA, if passed, would create a comprehensive national data privacy and security bill. The bill would cover any entity that collects, processes, or transfers covered data and is subject to the jurisdiction of the Federal Trade Commission (FTC). However, there are certain small business exemptions for businesses with less than $40 million of average annual revenue for the preceding three years and that do not collect personal data of more than 200,000 individuals or sell personal data of any individuals.

The bill would establish certain user rights that many states' businesses are already familiar with, including rights to access, correction, deletion, and portability, as well as the right to opt out of targeted advertising and data transfers. The bill would also require that consumers provide affirmative express consent for the transfer of "sensitive" data to third parties, with the definition of sensitive information broadly covering not only biometric and genetic data, but also information revealing online activities over time, such as that collected by cookies; calendars, texts, photos; information revealing individuals' access to or viewing of TV, cable, or streaming media services; and more.

The proposed legislation also includes a private right of action, allowing for civil litigation not only for data breaches but also for violation of numerous other provisions of the APRA, such as the requirement for affirmative consent regarding sensitive data. Moreover, where a term of service includes an arbitration provision, that could be deemed unenforceable for claims that allege a violation involving minors or that result in substantial privacy harm.

While the APRA would largely leave federal privacy laws untouched (e.g., GLBA, HIPAA, FCRA), it expressly preempts state privacy laws that regulate privacy issues covered by the APRA. Last year, the State of California opposed preemption in the ADPPA, calling on Congress to set the floor and not the ceiling of privacy regulation for states—and California's new Privacy Protection Agency recently announced its opposition to the APRA for the same reasons[4]. On the other hand, the APRA would largely replace the state-by-state patchwork of privacy laws, a list that grows longer each year.

The APRA includes a focus on artificial intelligence (AI). Covered entities would need to evaluate AI and use of algorithms, including to ensure they do not discriminate based on race, color, national origin, sex, or disability. The APRA would also include a right for consumers to opt out of covered algorithms and AI decisions.

4 *The California Privacy Protection Agency Opposes the American Privacy Rights Act,* California Privacy Protection Agency (June 26, 2024).

Interestingly, the proposed legislation appears to have been dealt a significant setback at the end of June when a scheduled markup meeting set to take place was cancelled after redlines were made to an updated draft of the regulation. The cancellation of the markup meeting following concerns that revisions to the law had substantially weakened certain protections leaves everyone with the same uncertainty that we have had for years about when, if at all, a federal privacy law may be passed.

California's Draft Risk Assessment and Automated Decision Making

In November 2023, the California Privacy Protection Agency (CPPA) released a set of draft regulations on risk assessments and the use of automated decision-making technology (ADMT). At its March 8, 2024 meeting, the Board of the CPPA moved, by a 3-2 vote, to advance proposed regulations addressing ADMT and risk assessments for the processing of personal information. The CPPA plays a crucial role in shaping and enforcing California privacy regulations that businesses need to follow, so while the proposed rules are still in development, businesses should pay close attention to their evolution. The CPPA's General Counsel Philip Laird said he expects the Board will vote to begin the formal rulemaking process for all three topics in July 2024, at the earliest. Once formal rulemaking begins, the Board has one year to finalize the regulations, per California's Administrative Procedure Act. A California appeals court recently ruled that the CPPA can immediately enforce rules as soon as they are finalized[5] which means businesses may not have meaningful lead time before enforcement commences once the CPPA finalizes risk assessment and ADMT regulations.

Automated Decision-Making Technology

The current draft of the regulations defines automated decision-making technology as any software or program that processes personal data and uses computation to execute a decision, replace human decision-making, or substantially facilitate human decision-making. The draft specifically notes that this definition includes software and programs "derived from machine learning, statistics, other data-processing techniques or artificial intelligence." The draft rules explicitly name some tools that do not count as ADMT, including spam filters, spreadsheets, and firewalls.

At its March 8 meeting, CPPA staff added a proposed definition for behavioral advertising to clarify and narrow the application of ADMT regulation on businesses[6] and to further provide guidance to businesses who may otherwise seek an exception from the risk assessment submission requirements[7].

The proposed regulations impose three main requirements on businesses using ADMT: (1) providing pre-use notices to consumers[8], (2) offering the right to opt-out[9], and (3) allowing access to information about ADMT use[10].

While these core elements remain unchanged since the December 2023 meeting, CPPA staff have made some business-friendly updates. These include narrowing the scope of certain requirements, tailoring pre-use notices to specific ADMT uses[11], and adding exceptions to opt-out provisions[12]. Additionally, they provided more flexibility in how information is presented and clarified some requirements with examples. However, the updated regulations also introduce new mandates, such as requiring businesses to disclose that they will not retaliate against consumers for opting out or requesting information about ADMT use.

5 *Are You Ready? CPRA Regulations Are in Effect Immediately: Attorney General Rob Bonta Wins a Reversal at the California Court of Appeals* (Feb. 13, 2024)

6 §7200(a)(2)
7 §7150(b)(3)(b)(iii)
8 §7220
9 §7221
10 §7222
11 §7220
12 §7221(b)

Risk Assessments

The draft regulations mandate that businesses conduct comprehensive risk assessments for various uses of personal information. They outline specific scenarios that will trigger the need for a risk assessment, including: selling or sharing personal information; processing sensitive information (a defined term that now includes the personal information of minors under the age of 16); using ADMT for making a significant decision concerning a consumer or for extensive profiling, such as employment or educational profiling, public profiling, or profiling for behavioral advertising; and using personal information to train ADMT or artificial intelligence that can be used for certain purposes. Notably, the risk assessment regulations will require organizations to conduct assessments before they use ADMT. Risk assessments will need to identify the risks that the ADMT poses to consumers, the potential benefits to the organization or other stakeholders, and safeguards to mitigate or remove the risk. These requirements are designed to align with global privacy standards, including the EU's General Data Protection Regulation (GDPR); however, it is not yet clear whether risk assessments for other jurisdictions will be transferable such that they would meet the demands of the final regulations on risk assessments.

In July 2024, the CPPA board voted against advancing draft regulations on cybersecurity audits, risk assessments, and ADMT to formal rulemaking. The board directed the CPPA staff to narrow the scope of processing activities that trigger obligations under the proposed regulations. The board plans to review revised drafts in September 2024. If approved then, the earliest these regulations could take effect is January 1, 2025. Meanwhile, the CPPA emphasized its enforcement priorities, including actions against improper data request practices and violations harming vulnerable populations.

Key Takeaways

Regardless of the final form of the regulations, the following things are certain: businesses will need to give detailed notices about their ADMT technology use, let consumers opt out, and conduct thorough risk assessments.

EU-U.S. Privacy Shield and International Data Transfers

The EU-U.S. Privacy Shield was originally established to facilitate the transatlantic exchange of personal data for commercial purposes, ensuring that adequate data protection standards were maintained between the European Union and the United States. However in July 2020 this framework was invalidated by the Court of Justice of the European Union (CJEU) in a landmark case known as "*Schrems II*." In its ruling on that case, the Court raised concerns about U.S. surveillance practices and their compatibility with EU privacy rights as reasoning for its annulment of the Privacy Shield. In the wake of the Privacy Shield's collapse, companies found themselves turning to alternative lifelines: Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs). But these were not simple plug-and-play solutions. Firms adopting these methods faced the onerous task of scrutinizing data protection landscapes in recipient countries and bolstering safeguards to shield personal data. As businesses grappled with this new reality, officials on both sides of the pond got to work on a replacement framework.

The efforts to establish a new data transfer framework culminated in March 2022, when the EU and the U.S. announced a political agreement in principle on a new Trans-Atlantic Data Privacy Framework. This new initiative aimed to address the deficiencies identified in the *Schrems II* ruling by introducing enhanced safeguards, stronger oversight mechanisms, and improved redress options for EU citizens. Businesses looking to be certified under the new Trans-Atlantic Data Privacy Framework must meet several requirements to ensure compliance.

As a threshold matter, to be eligible for certification under the Privacy Shield, businesses must: 1) be subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DOT); and 2) commit to adhering to the Privacy Shield Principles, which include notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, and recourse, enforcement, and liability.

The eligibility criteria for certification are as follows:

Self-Assessment: Conduct an internal review to ensure compliance with the Privacy Shield Principles. This involves evaluating current data protection practices and identifying and addressing any gaps in compliance.

Developing a Privacy Policy: Draft a privacy policy that aligns with the Privacy Shield Principles. This policy should be publicly available and provide clear information on data processing activities, including the type of data collected, purposes of processing, and third-party sharing practices.

Implementing Necessary Measures: Establish procedures to handle personal data in compliance with the Privacy Shield requirements. This includes implementing security measures to protect personal data from unauthorized access and breaches and ensuring data minimization, meaning only collecting and retaining data necessary for the intended purpose.

Designating a Privacy Officer: Appoint a privacy officer responsible for overseeing compliance and handling data protection issues. This officer will ensure adherence to the Privacy Shield Principles and act as a point of contact for data protection inquiries and complaints.

Selecting an Independent Recourse Mechanism: Choose an independent recourse mechanism to address complaints and disputes arising under the Privacy Shield. Inform individuals about the mechanism and how to access it. Common options include participating in programs provided by third-party privacy organizations and engaging with European data protection authorities.

Self-Certifying to the Department of Commerce: Prepare the required certification documentation and submit it to the U.S. Department of Commerce. This involves submitting a detailed report by a corporate officer, including information about the organization's data processing activities and privacy policies, paying the certification fee, and providing the necessary information to demonstrate compliance with the Privacy Shield Principles.

Key Takeaways

The terrain of international data transfers remains in a state of flux, demanding that businesses stay alert and nimble to successfully navigate the new framework's intricacies. Organizations must take a big-picture view of data protection. This means not only adhering to current rules but also keeping an eye on the horizon for emerging standards. By weaving both into their strategies, companies can create a robust approach that stands the test of time and scrutiny.

The Growing Landscape of Privacy Laws for Children

Over the past year, there have been significant developments in children's privacy laws at both the federal and state level. Businesses should continue to monitor these changes to ensure compliance, particularly given that the state laws described below are either currently in effect or expected to go into effect imminently, and more states are likely to follow suit with similar privacy laws for children. For example, California's enforcement agency, the CPPA, recently announced in June 2024 a public settlement with a video gaming company for its Children's Online Privacy Protection Act (COPPA) violations.[13]

FTC's Proposed Changes to the Children's Online Privacy Protection Act ("COPPA")

In December 2023, the FTC proposed revisions to the COPPA Rule, which was last updated in 2013. The FTC's proposals address recent developments in technology and impose new restrictions on a business's use and disclosure of children's personal information. Some of the FTC's proposed changes include:

- Requiring separate opt-in parental consent for targeted advertising;
- Prohibiting businesses from conditioning a child's participation in an online activity on the collection of their personal information;
- Prohibiting businesses from using online contact information and persistent identifiers to send push notifications to children to prompt or encourage them to use their service more;
- Strengthening data security requirements by mandating that businesses implement a written children's personal information security program that contains safeguards for protecting personal information collected from children;
- Limiting a business's data retention for only as long as necessary to fulfill the specific purpose for which it was collected; and,
- Expanding the definition of personal information to include biometric identifiers.

State Privacy Laws

In addition to the FTC's proposal, a patchwork of state-level initiatives has been enacted to address growing concerns about children's privacy. Many of these laws broaden the scope of data privacy protection for children in several key ways:

- States are expanding the definition of "child" to include children under the age of 18. Currently, under various laws, "child" is defined as under the age of 13 or 16.
- States are not only focused on websites that are specifically directed to children. Even websites meant for adults may be subject to children's privacy laws, if, for example, they are likely to be accessed by children.[14]
- States are regulating broader categories of personal information, such as precise geolocation information and biometric information.

13 For more information about the public settlement, please see *The California Privacy Protection Agency is Ramping up Enforcement* on page 20.

14 These state laws are much broader than the federal privacy law COPPA, which is limited to operators of websites "directed to children" under 13, or with "actual knowledge" that a website is collecting personal information of children under 13.

- States have imposed a range of requirements, such as obtaining a child's consent (or the consent of their parent/legal guardian if they are under the age of 13) before collecting, selling, or sharing their personal information, completing data privacy impact assessments, and prohibiting the use of dark patterns to encourage minors to provide their personal information.

California Children's Data Privacy Act

In January 2024, California introduced the Children's Data Privacy Act (AB 1949), a bill that would further amend the California Consumer Privacy Act (CCPA) to prohibit businesses from collecting the personal data of individuals under the age of 18, unless they receive affirmative authorization (i.e., opt-in consent) from the child. For children under the age of 13, the affirmative authorization must come from the child's parent or guardian.

Beyond restricting the collection of minor data, AB 1949 would also prohibit the "use or disclos[ure]" of personal information of minors without affirmative consent by the consumer or guardian. (Proposed amendment to Cal. Civil Code § 1798.121(e)). The law would also require the California Privacy Protection Agency to issue regulations to establish technical specifications for an opt-out preference signal and regulations regarding age verification.

AB 1949 has not been enacted into law as of the date of this publication, although it has passed the California Assembly.

To learn more about AB 1949, please visit our prior article, *California AG Proposes New Amendments To CCPA with the Children's Data Privacy Act*.

California Age-Appropriate Design Code

California's Age-Appropriate Design Code Act ("CAADCA") offers a more stringent set of protections than AB 1949. While ongoing litigation has temporarily blocked CAADCA's enforcement, businesses may eventually have to deal with this stricter law or some modified version of it.

CAADCA applies to businesses that provide online services, products, or features that are "likely to be accessed by children" who are under the age of 18. Whether a website is "likely to be accessed by children" will be determined based on various factors, including whether it is directed to children, routinely accessed by a significant number of children, has advertisements marketed to children, has design elements that are known to be of interest to children (i.e., games, cartoons, music, and celebrities who appeal to children), and has a significant audience that is determined to be children.

Additionally, CAADCA requires covered businesses to perform data protection impact assessments and implement stricter default privacy settings and terms. It imposes restrictions on collecting, selling, sharing, or retaining personal information of children for any reason other than the reason it was collected, and collecting, selling, or sharing children's geolocation information. CAADCA also prohibits the use of dark patterns to encourage minors to provide personal information and prohibits using a child's personal information in a way that is "materially detrimental to the physical health, mental health, or well-being of a child."

To learn more about CAADCA's requirements, please visit our prior article, *How To Prepare For California's New Privacy Law For Children*.

Non-California States

Several states outside of California have also passed laws regulating children's privacy. Some key components of these laws are summarized as follows:

Connecticut *(effective October 1, 2024)* – In June 2023, Connecticut amended its Data Privacy Act to impose restrictions on businesses that offer an online service, product, or feature to children under the age of 18. The law requires businesses to exercise a duty of care to avoid imposing a heightened risk of harm to minors. The law also mandates that businesses obtain the minor's consent, or the consent of a parent or legal guardian for minors below 13, to sell their personal information or engage in targeted advertising and profiling. Businesses must conduct data protection impact assessments.

Florida – In May 2023, Florida enacted the Florida Digital Bill of Rights. This law applies to "online platforms" that provide an online service, product, game, or feature likely to be predominantly accessed by children under the age of 18 (i.e., social media platform, online game, or online gaming platform). These online platforms are prohibited from collecting a minor's personal information if it might result in substantial harm or privacy risk to a minor; profiling minors (except under limited circumstances); and collecting, selling, or sharing any precise geolocation data of a child unless it is strictly necessary for the online platform to provide the service. Similar to CAADCA, the Florida law also prohibits using dark patterns to encourage minors to provide personal information.

Maryland *(effective October 1, 2024)* – In May 2024, Maryland enacted the Age-Appropriate Design Code Act. This law imposes a "best interests of children" duty of care for covered businesses when designing, developing, and providing products reasonably likely to be accessed by children. It also requires businesses to complete a data protection impact assessment; change all privacy settings provided to children to a "high level of privacy"; and bars processing of children's precise geolocation data by default.

New York *(effective June 20, 2025)* – In June 2024, New York enacted the Child Data Protection Act, which regulates data collection and targeted advertising related to minors. The law prohibits online sites from collecting, using, sharing, or selling personal data of anyone in New York under the age of 18, unless doing so is strictly necessary for the purpose of the website or the operator of the site receives informed consent from the user.

Colorado *(effective October 1, 2025)* – In May 2024, Colorado amended the Colorado Privacy Act to add protections for children's data privacy. The law creates new obligations for entities that offer any online service, product, or feature to minors (defined as under 18). The amendment is modeled after Connecticut's data privacy law.

Key Takeaways

Given the growing trend in children's data privacy laws across the country, businesses should continue to monitor these developments to determine whether they are subject to these laws and, if so, prepare to implement any changes required by them.

Privacy Litigation Trends

This year, we have seen a continued wave of privacy litigation. Three active areas of litigation include (1) data breaches, especially in the class action context, (2) wiretapping/eavesdropping cases brought against chatbots and activity-monitoring tools, including Meta Pixel and other analytics, and (3) cases brought under Section 638.51 of the California Invasion of Privacy Act ("CIPA") under a novel "pen register" theory.

Data Breach Litigation

Data breaches have continued to occur at a large scale in 2024, and we can expect to see more breaches and more resulting litigation in this area throughout the year. Additionally, circuit splits regarding the injury sufficient to establishing standing continues to fuel litigation even where actual misuse of breached data has not occurred. In particular, AI and machine learning developments continue to rapidly evolve the cybersecurity landscape in both positive and negative ways. While powerful AI and machine learning tools are being developed to aid in cyber-defense, they can also be used by hackers and threat actors to identify and target vulnerabilities. We expect to see continued litigation on this front, particularly in the class action context, throughout 2024 and beyond.

CIPA Litigation

This year has seen continued CIPA litigation as well. Lawsuits against companies for their failure to disclose that their chatbots and recording devices are recording or capturing the conversations continue to proliferate. While it seems intuitive that consumers do not have any right to privacy as to any conversations they are having with a company's chatbot, webchat, or any other devices, courts have allowed lawsuits as to these devices to proceed past the pleading stage under state wiretapping statutes, reasoning that consent from the user has not been obtained.[15] Accordingly, companies are advised to provide explicit written disclosure at the outset of any recording or chat sessions, explicitly stating that continued interaction with the program constitutes consent. For more information on compliance, please see our previous article, *Companies Should Keep in Mind Chatbots, Session Recordings, Mouseclicks: New Consumer Privacy Suits Continue Under Decades-Old Wiretapping Statutes*.

Companies have also continued to be sued for use of certain website analytics tools like Meta Pixel, Tik Tok Pixel, and others, and companies should take inventory of all website cookies and tracking tools being used on their websites in order to assess risk and take steps to reduce risk of litigation.

Pen Register/Trap-and-Trace Litigation

One novel theory that has arisen this year has been claims under the Pen Register Provision, Section 638.51. Section 638.51 of CIPA was initially enacted in 1967 to regulate the use of pen registers and trap and trace devices, which could track signals from outgoing and incoming calls, respectively, to obtain the involved phone numbers. Now, plaintiffs have been attempting to apply CIPA to websites' use of

15 The Federal Wiretapping Act, the Electronic Communications Privacy Act, is a one party consent statute. Accordingly, consent can be obtained by the company.

technology such as cookies, pixels, and analytics to track their users' website activity. One attractive aspect of this rule for plaintiffs is its $5,000-per-violation statutory damages.

Last year, plaintiffs were emboldened by a district court's decision to allow such a claim to survive past the motion to dismiss stage in *Greenley v. Kochava*, 2023 WL 4833466 (S.D. Cal. July 27, 2023). In *Greenley*, plaintiffs asserted CIPA violations against a data broker company that provided a software development kit to application developers, who could embed the kit into their mobile applications to deliver targeted advertising while tracking user locations, spending habits, and other information. The court in *Greenley* reasoned that this unique software's purported ability to collect a wide range of information could fall within CIPA's broad definition of a "pen register."[16]

More recently, two conflicting rulings by the Los Angeles County Superior Court have illustrated that the path forward is not so clear. In both *Licea v. Hickory Farms LLC* and *Levings v. Choice Hotels International, Inc.*, the plaintiffs alleged that the respective defendants violated CIPA by secretly deploying spyware that accesses visitor devices, installs tracking software, and tracks visitor browsing habits, i.e. obtaining users' IP addresses. On March 13, 2023, the court in *Hickory Farms* sustained a demurrer with leave to amend, finding that the complaint did not (1) establish that an IP address is equivalent to the "unique fingerprinting" in *Greenley*; (2) allege that the "device" at issue was a mobile phone or other form of potentially qualifying communication device; and (3) allege a lack of consent to the collection of IP addresses. A few weeks later, another judge overruled Choice Hotels' demurrer in a nearly identical case, reasoning that (1) Levings sufficiently alleged a pen register for purposes of the pleading stage; and (2) "if merely visiting a website constitutes consent to the use of a pen register, then Section 638.51(a) would be a dead letter. It could never be violated." It will be interesting to see how California courts continue to navigate this type of CIPA claim.

Key Takeaways

The wave of privacy litigation has not abated, particularly in the areas of data breaches, chatbot recordings, website analytics, and the application of Section 638.51 of the California Invasion of Privacy Act (CIPA) to modern tracking technologies. It's imperative that businesses stay vigilant as data breaches continue to result in class action lawsuits, driven by the rapid advancements in AI and machine learning which both aid and challenge cybersecurity efforts. Companies must also ensure that any use of chatbots or recording devices includes explicit user consent to avoid litigation under state wiretapping statutes. Additionally, the evolving interpretation of CIPA now requires that all companies carefully assess the risk of their website tracking technologies. We recommend reviewing your online and offline data collection practices and consulting with legal counsel to update privacy policies and develop compliance strategies to mitigate these legal risks.

16 *You've Worked to Make Your Website Cookies, Pixels, and Chat Function Compliant with Privacy Laws; Now What is a "Pen Register"* (Jan. 19, 2024).

Trends in Reproductive Health Privacy Post-*Dobbs*

Two years in the wake of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, we continue to see reproductive healthcare privacy developments at the state and federal levels.

At the federal level, the U.S. Department of Health and Human Services' Office for Civil Rights ("OCR") issued a Final Rule to modify the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule to protect reproductive health care access and privacy. The rule strengthens HIPAA by prohibiting the use or disclosure by regulated entities of protected health information related to lawful reproductive health care under certain circumstances, and, among other things, creating a rebuttable presumption that where reproductive health care was provided by a person other than the covered entity receiving the information request, the health care was lawful under the circumstances in which it was provided. The rule requires compliance by December 23, 2024.

Multiple states have reproductive health data protections either enacted or coming into effect this year, either as part of targeted legislation or included in larger data privacy laws. Among the protections put in place, we are seeing restrictions in the form of limitations on collecting, selling, and sharing reproductive health data, consumer consent requirements for the collection and use of reproductive health data, and geofencing restrictions in areas surrounding health care facilities.

Washington's My Health My Data Act and Nevada's Senate Bill No. 370, which both largely came into effect on March 31, 2024, involve similar protections for consumer health data, which they define to include reproductive health data. Both acts impose consumer consent requirements for the collection and sharing of consumer health dataand certain geofencing restrictions near health care facilities.

On September 27, 2023, Governor Gavin Newsom signed two bills amending the California Confidentiality of Medical Information Act ("CMIA") into law in California. Assembly Bill ("AB") 352 strengthens privacy protections for electronic medical records related to abortion and abortion-related services, gender affirming care, and other sensitive services. AB 254 includes protections for digital data pertaining to reproductive and sexual health in personal health tracking applications.

Most recently, Maryland enacted the Maryland Online Data Privacy Act ("MODPA") on May 9, 2024. The MODPA, which takes effect on October 1, 2025, protects consumer health data, which is defined to include data related to reproductive or sexual health care, as sensitive data. It imposes restrictions on parties covered by the act, including prohibitions on collecting, processing, or sharing sensitive data unless strictly necessary to provide or maintain a specific product or service requested by the consumer, and on selling sensitive data. The Act also requires covered parties to provide consumers with a privacy notice describing, among other things, the categories of sensitive data collected and shared, and restricts geofencing within 1,750 feet of mental health, sexual health, or reproductive health facilities.

We will continue to monitor these developments at both the state and federal level.

Navigating CAN-SPAM Compliance:
Essential Tips for Protecting Privacy in Marketing Emails and Texts

In the age of digital marketing, reaching out to customers via email and text messages is a powerful tool. However, ensuring compliance with the CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography And Marketing) is crucial not only for legal reasons but also to protect the privacy of your customers. Here are essential tips to keep in mind to help you navigate CAN-SPAM regulations whenever you send out any marketing blasts—either through email or text.

Consent: Make sure you have a consumer's consent before sending them a marketing email.

Clear and Accurate Identification of the Sender: There should be accurate and recognizable "from" names disclosed so the consumers know who is sending the communication.

Honest Subject Lines and Message Content: Avoid using clickbait or misleading language. Have honest and transparent messages.

Disclosure of Advertisements: Clearly and conspicuously identify the message as an advertisement or solicitation.

Providing a Physical Address: Under CAN-SPAM, all marketing e-mails must provide a physical address; this is not required for text messages, however.

Providing an Opt-Out Mechanism, and Promptly Honoring that Opt-Out Mechanism: Provide a clear and conspicuous explanation of how the recipient can opt out of receiving email from the company in the future. Include either a return email address or another easy online mechanism (such as an "unsubscribe" link) that the recipient may use to choose to opt out. For text messages, advise consumers that texting "STOP" will be a sufficient opt-out. More importantly, you should have mechanisms in place to promptly honor those opt-outs when they are requested.

Regular Compliance Audits and Monitoring Third-Party Marketing: It is advised to consistently check in with your marketing team or the vendor who is handling your marketing. Non-compliance can rack up hefty fees per violation.[17]

Key Takeaways

Complying with the CAN-SPAM Act is not just a legal requirement but also a best practice for protecting customer privacy. By following these tips, you can effectively manage your email and text message marketing campaigns, ensuring they are both effective and respectful of privacy. Transparency, honesty, and respect for your recipients' preferences are key to successful and privacy-conscious digital marketing.

17 For example, for a CAN-SPAM e-mail violation, the penalties could be up to $51,744 *per violation*. See also *CAN-SPAM Act: A Compliance Guide for Business*.

The California Privacy Protection Agency is Ramping up Enforcement

Background on the California Privacy Protection Agency (CPPA) under California's Privacy Laws

The California Privacy Protection Agency (CPPA) is the regulatory body responsible for enforcing the CCPA, which grants California residents enhanced privacy rights and control over their personal information. Key provisions of the CCPA include the right to know what personal information is being collected, the right to delete personal information, the right to opt-out of the sale of personal information, and the right to non-discrimination for exercising these rights.

With the creation of the CPPA, all eyes were on the new enforcement agency and the direction they would go in enforcing California privacy rights. While there still have been only a few public settlements stemming from enforcement actions, the CPPA has issued a slew of public statements about the direction and attention of the Agency. Below are a few areas of law the CPPA appears to be turning its attention to.

Children's Data

The CPPA issued its most recent public enforcement action and settlement with an online gaming company, which included a $500,000 fine for violating various laws governing children's data. At issue was a video game, "SpongeBob: Krusty Cook-Off," which claimed that it was not directed at children under 13 and its terms of services said that children under the age of 13 should not use its services. Nevertheless, the CPPA found the application to be in violation of the Children's Online Privacy Protection Rule ("COPPA") along with various provisions of the California Consumer Privacy Act ("CCPA").

COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.[18]

Under COPPA, the CPPA found that the company at issue had "directed" its services to children 13 years of age or younger on the following grounds:

- the age screen that populated the application upon download was not provided in a neutral and effective manner;
- the age screen allowed children under 13 to consent to receiving advertising without verifiable parental consent; and,
- the application processed personal information of children who self-identified as under 13 without verifiable parental consent.

Under COPPA, "verifiable parental consent" is defined as "making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child: (1) receives notice of the operator's personal information collect, use, and disclosure practices; and (2) authorizes any collection, use, and/or disclosure of the personal information."[19]

18 15 U.S.C. § 6501-6508; *see also* 78 FR 4008.
19 78 FR 4008, § 312.2 (Definitions, "*Verifiable Parental Consent*").

Whether or not a website or service is "directed" towards children is a fact-intensive, comprehensive determination considering the "subjective matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as whether advertising promoting or appearing on the Web Site or online service is directed to children."[20]

The company was found to have violated COPPA because it was found to have "directed" its video game towards children and had actual knowledge that children under the age of 13 were engaging with the video game without the requisite parental consent.

Failure to Provide Adequate Out-Opts or Failing to Honor Opt-Outs Prior to Selling Consumer Data

While not under the CPPA, the California Attorney General's Office has separate enforcement power to effectuate and enforce California's privacy laws. The first was against beauty make-up giant Sephora in August 2022, for failing to process opt outs of users who did not want Sephora to sell their personal information. This included Sephora's failure to honor global opt-out controls.

The second was in February of 2024 against the food delivery company Doordash, settling allegations against Doordash for violations of the CCPA and the California Online Privacy Protection Act (CalOPPA). Doordash was alleged to have violated various privacy laws by selling consumer data without providing notice or an opportunity to opt out of the sale prior to the sale.

20 78 FR 4008, § 312.2 (Definitions, "*Web site or online service directed to children*").

Smart Vehicles and Employee Data

The CPPA issued press releases in 2023 indicating its intent to focus on smart vehicles and companies' employee collection practices. As to smart cars, the CPPA is particularly concerned with "vehicles . . . embedded with several features including location sharing, web-based entertainment, smartphone integration, and cameras."[21] Similarly, the CPPA issued another press release announcing that the CPPA, in an investigative sweep, sent inquiry letters to large California employers requesting information that these companies are complying with the CCPA, which was amended by the CPRA to include employee data.[22] This press release signaled that the expansion to give the same privacy rights consumers have to employees underlines that the CPRA amendments are not toothless and are not meant to be ignored.

Health Data Post-*Dobbs* and Other Sensitive Personal Information

With the recent decision in *Dobbs v. Jackson Women's Health Organization* overturning a federal constitutional right to abortions, California has turned towards protecting these rights along with other health rights rooted in a state-focused right to privacy. See our article, *Trends in Reproductive Health Privacy Post-Dobbs*, on page 18. This means that health data—which is already typically governed by a multitude of statutes including HIPAA, and is subject oftentimes to heightened scrutiny as sensitive personal information—will be afforded extra attention. California, to date, is still the only state that affords a privacy right of action if sensitive personal information, which oftentimes includes confidential health data, has been disclosed in a data breach.

21 *See* *CPPA to Review Privacy Practices of Connected Vehicles and Related Technologies* (July 31, 2023).

22 *See* *Attorney General Bonta Seeks Information from California Employers on Compliance with California Consumer Privacy Act* (July 14, 2023).

For companies who work in health-related fields, collect biometric information, and/or collect information that could pertain to an individual's health, it is advised to silo that information and provide additional security that you otherwise would not afford to non-sensitive personal information.

This means that health data—which is already typically governed by a multitude of statutes including HIPAA, and is oftentimes subject to heightened scrutiny as sensitive personal information—will be afforded extra attention.

Key Takeaways

While this may seem to be a hodgepodge of various enforcement actions, there are some key takeaways about California's eye of enforcement:

- The CCPA is paying attention to websites or mobile applications that attract a lot of children. Merely stating that your website or mobile application is not "intended" for children is insuff icient if you know that many children are actively engaging on your platforms.
- Continue updating your privacy policies to adequately disclose your collection practices, ensure any changes to your collection practices are adequately tracked to your internal data map, and honor all requests, including requests to stop selling or sharing.
- Review your collection practices, and to the extent you are collecting or processing sensitive personal information, ensure there are adequate safeguards, particularly regarding your practices with sensitive personal information.
- Ensure that global opt-out preference signals are honored. Global opt-out preference signals have been codified in the regulations.[23] This requires working with your IT team to ensure that your website can detect opt-out preference signals.
- While compliance with all privacy laws and regulations is always advised, we understand that companies have a barrage of various to-dos. If in doubt, prioritize the front-facing collection processes—such as consumer privacy policies, job applicant notices, and other low-hanging fruit that is publicly available for regulators to review.

23 *See* Title 11, Division 6, Art. 3 § 7025 (regulating opt-out preference signals).

Contact

If your company needs assistance with any privacy issues, the Coblentz Data Privacy and Cybersecurity attorneys can help. Please contact a member of the team below for further information or assistance.

Authors

Scott C. Hall

Head of Data Privacy and Cybersecurity Group
Partner
San Francisco

Contact
415.772.5798
shall@coblentzlaw.com

Mari S. Clifford

Associate
San Francisco

Contact
415.268.0504
mclifford@coblentzlaw.com

Sabrina A. Larson

Partner
San Francisco

Contact
415.268.0559
slarson@coblentzlaw.com

Emily Lentz

Associate
San Francisco

Contact
415.268.0559
elentz@coblentzlaw.com

Amber Leong

Associate
San Francisco

Contact
415.268.0535
aleong@coblentzlaw.com

Bina Patel

Associate
San Francisco

Contact
415.268.0563
bpatel@coblentzlaw.com

Coblentz Patch Duffy & Bass LLP
One Montgomery Street, Suite 3000
San Francisco, CA 94104

coblentzlaw.com