troutman pepper

2023 Privacy Year in Review

Privacy + Cyber and Regulatory Investigations, Strategy + Enforcement (RISE) Practices

troutman.com

Table of Contents

INTRODUCTION

Looking at 2023, the landscape of privacy, security, and artificial intelligence was nothing short of dynamic. The year was marked by significant growth across various sectors, including business, data, legal frameworks, and investigative and enforcement actions. This growth was paralleled by an increase in data usage, the advent of new technologies, and a surge in cyber threats and breaches.

To provide an overview of these developments, our Privacy + Cyber and Regulatory Investigations, Strategy + Enforcement (RISE) practices joined forces to produce this Year in Review. Our aim is to help you navigate the complexities of the past year and prepare for the challenges and opportunities that lie ahead.

This document is structured in two sections. The first offers a strategic overview of global trends, themes, risks, and best practices across the international landscape. The second section delves deeper, spotlighting notable cases that may have been overlooked, with a particular focus on emerging technologies and U.S. state attorneys general enforcement and litigation.

While we've highlighted the key trends and developments that we believe will shape 2024, we understand that each reader may have unique questions and concerns. Please reach out to us with any queries you may have.

Best wishes to you for a year filled with happiness, health, privacy, and security.

James Koenig
Partner, Co-Chair - Privacy + Cyber Practice

Stephen C. Piepgrass
Partner, Co-Leader - Regulatory Investigations, Strategy + Enforcement Practice

Ronald I. Raether, Jr.
Partner, Co-Chair - Privacy + Cyber Practice

Ashley L. Taylor, Jr.
Partner, Co-Leader - Regulatory Investigations, Strategy + Enforcement Practice

CONTRIBUTORS

James Koenig
Partner
jim.koenig@
troutman.com
610.246.4426

Samuel E. “Gene” Fishel
Counsel
gene.fishel@
troutman.com
804.697.1263

Stephen C. Piepgrass
Partner
stephen.piepgrass@
troutman.com
804.697.1320

Joel M. Lutz
Counsel
joel.lutz@
troutman.com
404.832.6007

Ronald I. Raether, Jr.
Partner
ron.raether@
troutman.com
949.622.2722

Zie Alere
Associate
zie.alere@
troutman.com
804.697.1343

Ashley L. Taylor, Jr.
Partner
ashley.taylor@
troutman.com
804.697.1286

Karla Ballesteros
Associate
karla.ballesteros@
troutman.com
949.622.2415

Joshua D. Davey
Partner
joshua.davey@
troutman.com
704.916.1503

Rachel Buck
Associate
rachel.buck@
troutman.com
704.916.1512

Kim Phan
Partner
kim.phan@
troutman.com
202.274.2992

Carson A. Cox
Associate
carson.cox@
troutman.com
804.697.1338

Angelo A. Stio III
Partner
angelo.stio@
troutman.com
609.951.4125

Natasha E. Halloran
Associate
natasha.halloran@
troutman.com
804.697.1296

Natalia A. Jacobo
Associate
natalia.jacobo@
troutman.com
213.928.9821

Marnishia L. Jernigan
Associate
marnishia.jernigan@
troutman.com
213.928.9848

Namrata Kang
Associate
namrata.kang@
troutman.com
202.274.2862

Robyn W. Lin
Associate
robyn.lin@
troutman.com
949.622.2447

Susie Lloyd
Associate
susie.lloyd@
troutman.com
704.916.2370

Alexandria Pritchett
Associate
alexandria.pritchett@
troutman.com
858.509.6088

McKayla Riter
Associate
mckayla.riter@
troutman.com
804.697.1486

Whitney L. Shephard
Associate
whitney.shephard@
troutman.com
617.443.3709

Trey Smith
Associate
trey.smith@
troutman.com
804.697.1218

Edgar Vargas
Associate
edgar.vargas@
troutman.com
949.622.2473

Daniel Waltz
Associate
daniel.waltz@
troutman.com
312.759.5948

Laura E. Hamady
Senior Privacy & Security Advisor
laura.hamady@
troutman.com
312.759.8880

Mac McCullough
Senior Privacy & Security Advisor
mac.mccullough@
troutman.com
312.759.3650

I. 2023 KEY TRENDS: 15 THINGS COMPANIES ARE DOING NOW TO PREPARE FOR 2024 AND BEYOND

Key Trend: New U.S. State Comprehensive Privacy Laws Gaining Momentum at 13 and Counting

During the 2023 legislative session, seven states passed comprehensive consumer privacy laws, with New Jersey enacting its own in January 2024, leaving the U.S. with a total of 13 separate comprehensive laws that will take effect over the next two years,[1] in addition to a battery of privacy-adjacent laws regulating, among other things, consumer health, children's privacy, artificial intelligence (AI) use cases, and rules for operators of social networks. Though these laws share many of the same underlying requirements, they all contain unique elements that companies will need to evaluate when updating their compliance programs. For example, some but not all states require organizations to conduct data protection assessments, and many states have distinct requirements for handling certain consumer privacy requests.

What companies are doing now

1. **Review and Update Online Privacy Notices.** Companies that have not already conducted an update of their online privacy notices in 2023 should do so now as well as undertake at least an annual review of their privacy notices to ensure that evolving state requirements are captured in their disclosures and that their data practices are up to date and accurate going forward.

    - **Pro Tip:** Companies should ensure that their privacy notices reflect the most current state of their uses of technologies, outputs, or services that employ artificial intelligence and advertising technology (AdTech) and/or process sensitive personal data, including location data, biometric and health data, and children's data, and data sharing activities, as these are likely to be a focus for regulators in 2024.

    - See Privacy, Cyber and AI Digest (Digest) section on New U.S. State Comprehensive Privacy Laws for a deeper comparison of the distinctions between the various state laws.

    - Below are some examples of our thought leadership on this topic:

        - CCPA/CPRA Will Apply to Employee AND B2B Data — Five Steps to Prepare for the January 1, 2023 Effective Date
        - Washington Legislature Goes Big With "My Health My Data Act"
        - California Age-Appropriate Design Code Is Not Child's Play: Five Practical Tips to Comply and Protect Kids' Privacy
        - CPRA-Part-3-of-5-Daily-Journal.pdf

2. **Develop and Post an Employee and Applicant Privacy Notice.** While the California Consumer Privacy Act (CCPA) required worker and applicant privacy notices as of January 1, 2020, many companies did not put such policies in place, as California delayed the application and enforcement of worker and applicant rights. As of July 1, 2023, that changed, and the CCPA extended privacy rights to workers and individuals in their business capacities, requiring companies with job applicants, workers, and business contacts in California to honor privacy rights requests from these populations. In 2023, some companies elected to revise their general online privacy notice to include specific provisions for employees,

[1] Additionally, Florida passed a data privacy law, but its high threshold for applicability makes it largely inapplicable to many businesses.

but most companies chose to maintain a separate privacy notice specifically for their workers and applicants due to the often-distinct ways companies use this data. In many cases, global companies create integrated global worker and applicant policies to drive parity where possible and practical (and we recommend that).

- See Digest section on New U.S. State Comprehensive Privacy Laws for a deeper discussion on privacy rights notice to individuals.
- Below are some examples of our thought leadership in this area:
  - Privacy Parade: How to Navigate the Rush of New State Privacy Laws
  - CCPA/CPRA Will Apply to Employee AND B2B Data — Five Steps to Prepare for the January 1, 2023 Effective Date
  - CPRA-Part-3-of-5-Daily-Journal.pdf

3. **Update and Expand the Scope of Privacy Risk Assessments.** As noted above, with a handful of exceptions, U.S. state laws increasingly require organizations to conduct data protection impact assessments (DPIAs) for potentially high-risk data processing activities. While companies that have been subject to the European General Data Protection Regulation (GDPR) are leveraging their existing DPIA processes, most organizations are creating new or updating existing risk assessments to create "integrated impact assessments" that cover GDPR, the detailed guidance of California and Colorado, as well as security risks and evaluations of new artificial intelligence use cases.

   Companies using this new programmatic and integrated approach to evaluating new technologies and/or data risk are better situated to adapt to changing areas of regulation. For example, companies that work with health data might perform a DPIA pursuant to Washington state's My Health My Data Act,[2] and then be spurred into drafting a separate health data privacy policy. Similarly, a company might perform an assessment of the risks associated with its collection and processing of children's data (in connection with California's Age-Appropriate Design Code and similar laws that could become effective in 2024),[3] and use the results of such assessment to build in new protections and privacy controls to benefit all end users.

   - See the discussion of business obligations in the Digest section on New U.S. State Comprehensive Privacy Laws for a deeper analysis on DPIAs. As an example of our thought leadership in this area, see California ADCA bill aims to increase children's data privacy | Security Magazine.

Key Trends: Increased Scrutiny of Lead Generation Activities and Data Brokers Impacting Marketing for All Companies

2023 brought an increased focus on data brokers (and companies that could be considered data brokers) at the state and federal level. Some U.S. states enacted or amended data broker laws, and the Consumer Financial Protection Bureau (CFPB) initiated rulemaking that proposes to apply Fair Credit Reporting Act (FCRA) principles to many businesses and use cases that do not meet the FCRA's definition of a credit reporting agency (CRA). In addition, the Federal Communications Commission (FCC) adopted new rules that change the definition of prior express consent under the Telephone Consumer Protection Act (TCPA). When

[2] Washington's My Health My Data Act is a comprehensive health privacy law that imposes broad restrictions on how "consumer health data" can be used by companies doing business in the state of Washington or engaging with Washington residents. See Washington Legislature Goes Big With "My Health My Data Act." Nevada passed a similar law in 2023 also focusing solely on health data privacy. See Nevada Consumer Health Data Bill Signed into Law (hipaajournal.com).

[3] Though enforcement of the California Age-Appropriate Design Code Act is currently blocked pursuant to a preliminary injunction by the Northern District of California, other states are actively pursuing the passage of similar bills while the case is ongoing. See California Age-Appropriate Design Code Is Not Child's Play: Five Practical Tips to Comply and Protect Kids' Privacy.

implemented, these amendments will limit the practice of relying on a single consumer consent to authorize robotexts and robocalls from multiple marketers - a common practice of comparison-shopping services and lead generation businesses. These changes will significantly alter the economics and compliance practices of the data ecosystem as it operates today.

What companies should do now

4. **Conduct a Quick Assessment to Understand If You Inadvertently Fall Under the Expanded Definitions of Data Brokers.** Organizations that have not traditionally been considered or regulated as data brokers should understand whether the new state laws or proposed new CFPB definitions affect them. All companies should also revisit their data maps to identify whether and which data sources may come from brokers and how the CFPB's proposed rulemaking plans may impact their business and shift their compliance obligations.

5. **Register as a Data Broker if Necessary, and Understand the Applicable Exemptions.** Organizations that are already regulated as data brokers should ensure that they are registered in each of the four states – Vermont, California, Texas, and Oregon – that now have data broker registration requirements. California data brokers should also understand the sweeping implications of *The Delete Act*, the state's 2023 amendment that requires data brokers to respond to a central, state-operated mechanism through which consumers could centrally request deletion of their data. Though this central mechanism may not be operable for two years, understanding potentially applicable exemptions and other business impacts well in advance will avoid unnecessary costs and operational impediments for brokers subject to these laws.

6. **Develop and Update Procedures for Licensing and Sourcing Third-Party Leads and Marketing Playbooks.** Though the FCC's new rules amending the TCPA will likely not become effective until mid to late 2024, companies that provide lead generation or comparison-shopping services will need to redesign their lead collection practices in states where express consent is within the new rules' purview (for example, by facilitating direct contact between the consumer and a potential seller or allowing a consumer to select and consent to specific sellers). Companies that use robotexting and robocalling, particularly those that rely on lead generation services for their marketing activities, should implement procedures to validate that individuals have provided legally appropriate consent before they may receive marketing communications, particularly if contact with the consumer will be made after the rules go into effect. Also, increasingly, companies are creating integrated marketing privacy compliance playbooks with policies, procedures, training, and model contract provisions covering marketing activities by email, telemarketing, robocalls, texting, social media, mail, kiosk, online/scraping, faxing, and other forms of direct marketing.

- See Digest section on Developments in the Consumer Data Ecosystem, Data Brokers in the Spotlight for a deeper discussion on this topic.
- Below are some examples of our thought leadership in this area:
  - CFPB Outlines Rulemaking Plan to Dramatically Alter Decades of FCRA Requirements for Everyone in the Consumer Data Ecosystem | Consumer Financial Services Law Monitor
  - FCC Closes Lead Generator Loophole by Requiring One-to-One Consent; Proposes Further Regulation of Robocalls/Robotexts | Consumer Financial Services Law Monitor
  - FCC Proposes New Rules for Revocation under the TCPA | Consumer Financial Services Law Monitor

Key Trend: New Restrictions, Enforcements, and Class Action Liabilities for Cookies and Other Tracking and AdTech

While the FTC has been active in enforcements regarding AdTech and dark patterns opt-outs (e.g., GoodRx and Epic Games), all comprehensive state privacy laws to date have required covered businesses to provide consumers with an opt-out mechanism for the use of their personal information for certain types of targeted advertising. Many of the states also require businesses to recognize browser-based opt-out mechanisms as ways for consumers to opt out of sales and/or sharing. In conjunction with these requirements, session replay, wiretapping, and AdTech have drawn increased regulatory scrutiny and attracted high volumes of litigation from the plaintiffs' bar, including through claims based on old laws, such as the 1988 Video Privacy Protection Act.

What companies should do now

7. **Conduct an Inventory and Audit of Cookies and Other Tracking Technologies, Especially on Sites That Offer Video Content.** Companies that use AdTech and display videos on their websites should revisit their use of cookies and tracking technologies to understand what each technology does and ensure that their privacy policies accurately disclose these uses. Companies should also understand when and how the technologies fire and consider using a consent preference management tool to provide consumers with the rights and options available to them in their respective jurisdictions. In particular, many companies have come under fire from the plaintiffs' bar for their use of tracking technologies on sites that provide paid or subscription-based video content, so special care should be taken to provide end users with choices regarding tracking on such services.

8. **Leverage Emerging Technical Solutions and Safe Harbors for Digital Technologies.** Companies should have procedures, standards, and guidelines governing the use of cookies, pixels, and SDKs that align with established frameworks such as the NIST Privacy Framework, the Privacy Management Framework, and the Fair Information Privacy Practices. Additionally, companies should identify APIs or alternative technological tools that can be employed and built out within existing operational and technical platforms, and/or adopt technical controls that can be used to automate tracking and notification processes, for example, by utilizing standards, guidance, and best practices issued by the Interactive Advertising Bureau (IAB).

- See Digest section on New Restrictions and Liability for Online Advertising for a deeper discussion on this topic.
- Below are some examples of our thought leadership in this area:
  - Cookies and Online Tracking of Health Signals: An OCR Prescription for Potential Peril | Troutman Pepper
  - Ad Technology Compliance Tips From Video Privacy Claims | Troutman Pepper

Key Trend: Companies Stop Panicking and Develop AI Safeguards Leveraging Adjacent Privacy Controls

The past year saw dizzying global legislative activity that included broad regulation in the European Union and narrowly targeted U.S. municipal and state laws aimed at certain industry sectors. From the EU's AI Act to the publication of the NIST AI Risk Management Framework to the issuance of a sweeping executive order from the Biden administration to the publication of many position papers and statements from global regulators, we saw consensus around the need to regulate AI, but less agreement on how it should be governed or by whom.

What companies should do now

9. **Adopt an Ethical Data Collection, Use, and Sharing Charter for AI Governance and Training.** Many organizations are pulling together cross-functional governance committees to define and oversee the use of AI for internal and external uses in their business, starting with the publication of an effective AI use policy, workforce-wide training, and ongoing monitoring and oversight to ensure compliant use of these promising technologies.
10. **Update Data Protection Agreements (DPAs)/ License Agreements, Online Terms of Use (TOS), and Online Scraping Guidelines.** To ensure that they are not inadvertently making their sensitive, proprietary, confidential, or customers' data available to third parties and service providers, companies should review and consider broadening and updating their DPAs, licensing contracts, master service agreements, and terms of use documents to specifically address the use of data for AI-related model training and development. While an organization's internal AI policies will help most workers, instituting operational procedures that outline the collection and use of data (in particular, only training on data for which your organization has clear rights) can make the difference between wanting to comply and being compliant. For example, many companies find it helpful to maintain guidelines that specify exactly what and how third-party online content can be utilized, as well as implementing audit and post-generation checks to ensure the quality of AI-generated content.
11. **Address the Use of AI in Privacy and Information/Cybersecurity Policies.** As noted elsewhere, all companies should ensure that their external and internal privacy notices address how personally identifiable information will be gathered and protected when using AI tools. Information security/ cybersecurity policies should also be updated to identify safeguards that have been deployed to protect personal information when using AI tools or systems.
    - See Digest section on Artificial Intelligence for a deeper discussion on this topic.
    - Below are some examples of our thought leadership in this area:
      - AI: Technology, Opportunities, Risks, and Best Practices (Part Two)
      - Preparing for an Era of Regulated Artificial Intelligence
      - AI Use Policies

- Artificial Intelligence — From Risk to Reward: Key Questions to Address When Crafting Generative AI Usage Policies
- Will Generative AI, Including ChatGPT, Transform Businesses and Law Firms?
- Navigating the AI Landscape: Privacy, IP, Policies and More — An Industry Expert Roundtable
- Managing AI — Risk, Reward & Regulation! — AI Discrimination and Emerging Best Practices
- Ninth Circuit Provides Guidance on Web Scraping | Troutman Pepper

13. **Review Compliance Program Before Registering Under the EU-U.S. Data Privacy Framework (DPF).** The U.S. and EU made great strides in finalizing the DPF, sparking renewed interest in data transfer frameworks and agreements. U.S. businesses that previously self-certified under the Privacy Shield and want to renew their certifications may wish to undertake a fresh self-audit in advance of certifying and update their online privacy notices accordingly.
    - See Digest section on Developments in Global Privacy Law for an in-depth discussion on the EU-U.S. DPF.

Key Trend: New and Evolving Global Privacy Laws

Privacy has remained a global focus with more countries enacting or refining privacy laws and regulations. Canada, the United Kingdom, Brazil, Singapore, Vietnam, Japan, India, China, and others have continued to significantly adapt their laws and refine guidance in ways that require many companies to take stock of their business practices and data flows.

What companies should do now

12. **Review Data Flows and Update International Data Protection Agreements (DPAs).** Companies should establish or update their data inventory to reflect the types of data originating in and being exported from countries outside of the U.S., particularly those with demanding privacy obligations such as China's Personal Information Privacy Law (PIPL) and India's Digital Personal Data Protection Act (DPDPA). Leveraging these data maps, organizations should ensure that they are assessing their current obligations and reviewing and revising their DPAs at least annually to reflect evolving obligations and applicable exemptions, where available.

Key Trend: Ransomware and Wire-Transfer Fraud Continues Amid Heightened Scrutiny and Obligations

Security incidents only accelerated in 2023, with global incidents such as the MoveIT vulnerability capturing headlines and ransomware incidents leading to critical governmental shutdowns and consuming organizational resources. State and national regulators have consequently demanded more accountability and oversight of organizational security practices.

What companies should do now

14. **Review and Update Incident Management and Response Plans and Conduct Tabletops.** Organizations are increasingly aware that it is not a matter of if they are affected by a security event, but when and to what extent. As such, they are working to ensure that they have up-to-date incident management and response plans (IRM), including ransomware policies and connections with service providers (such as outside legal counsel and forensic experts) to be on call when the time comes. Public companies are also updating their IRM plans to reflect new rules promulgated by the

Securities and Exchange Commission (SEC), which require prompt disclosure of material cyber incidents to the SEC and in Form 8-Ks. Companies are also increasing the frequency and sophistication of tabletop exercises – sessions which test how their organizations respond to a security incident by simulating one unexpectedly – and using the learnings from these exercises to bolster their policies and on-call resources to be better prepared for a live event.

15. **Prepare Board Presentations and Cyber-Preparedness Report.** For public companies affected by the new SEC rules, companies should ensure they have refined their processes for assessing, identifying, and managing material risks and potential effects of cybersecurity threats, and ensure the full education, involvement, and oversight by the board of directors. Through the addition of Regulation S-K Item 106, companies will need to describe these governance processes as well as management's role and expertise in assessing and managing material risks from cybersecurity threats in their Form 10-K.
    - See Digest section on Notable Cyber-Related Policy Developments and Administrative Activity for a deeper discussion on new SEC cybersecurity disclosure rules for public companies.
    - Below are some examples of our thought leadership in this area:
        - SEC adoption of final cybersecurity rules
        - Navigating the Complexities of Regulatory Data Incident Investigations | Regulatory Oversight
        - SEC Adopts Final Cybersecurity Rules — Requires Companies to Focus on Their Security and Disclosure Plans
        - Your Organization Has Suffered a Data Incident: Now Here Are the Regulators It Will Likely Encounter

II. PRIVACY, CYBER, AND AI DIGEST

A. New U.S. State Comprehensive Privacy Laws

In 2023, seven additional states passed comprehensive consumer privacy laws, and in January 2024, New Jersey enacted its own, leaving the U.S. with a total of 13 separate comprehensive state laws that will come into effect over the next two years[4] and a battery of privacy-adjacent laws regulating, among other things, consumer health and children's privacy. The laws share many of the same underlying principles, including providing consumers with a set of privacy rights and imposing specific disclosure, security, and other obligations on businesses that handle personal information. While sharing many commonalities in structure, the laws diverge in their application both to businesses and to individuals, and by the nature of enforcement mechanisms and other remedies available for violations of these laws.

Scope

The comprehensive state privacy laws to date protect the personal information of consumers, with only California extending privacy rights to workers and individuals whose personal information is collected in their business capacities and imposing new disclosure obligations on businesses. These rights generally include the right of access, correction, deletion, portability, and the option to opt out of sale, targeted advertising, and profiling, depending on the state.

Applicability

Most comprehensive state privacy laws exempt nonprofits. However, Colorado, Oregon, and Delaware do not. Further, each law has additional thresholds of applicability and data level exemptions which are not uniform and will require careful analysis for organizations potentially subject to these laws' requirements. For example, Texas' law, unlike other state laws, does not set a monetary or personal information processing threshold for applicability of the law, but specifies it does not apply to "small businesses." Most state privacy laws provide an entity-level exemption for organizations regulated by Gramm-Leach-Bliley Act (GLBA), but Oregon and California's laws do not. Similarly, all comprehensive state privacy laws provide an entity-level exemption for organizations regulated by the Health Insurance Portability and Accountability Act (HIPAA) except for California, Colorado, Oregon, and Delaware, where only HIPAA-regulated data is exempt. These variances reinforce the importance for all organizations to understand the data they have and carefully evaluate the applicability of these state laws to their business.

Business obligations

Most of the comprehensive laws impose similar operational obligations on businesses to implement reasonable data security measures, supervise their service providers including through specific contractual provisions, minimize the amount of personal information they collect, and, increasingly, to conduct data protection assessments for potentially high-risk data processing. All laws enacted to date require businesses to disclose their privacy practices to consumers, and most require affirmative consent (which in some cases explicitly bars the use of "dark patterns") to process sensitive personal information and fairly honor individual rights requests (including, increasingly, by recognizing universal opt-out mechanisms) and appeals. While some states, such as California and Colorado, have promulgated detailed regulations to guide businesses in their compliance, most have not.[5] For many organizations seeking to operate and maintain a comprehensive privacy program, having

[4] Additionally, Florida passed a data privacy law, but its high threshold for applicability makes it largely inapplicable to many businesses.

[5] Florida also requires the promulgation of regulatory guidance but is subject to the limitations noted in footnote 4.

common baselines across the laws is a comfort but will not alleviate the need to respond to the detailed provisions in these various regulations and to analyze each law for specific requirements and exemptions that may apply to their industry sector and individual business practices.

Enforcement

All of the comprehensive state privacy laws provide for enforcement by the attorney generals' office, with the exception of California's, which empowers the California Privacy Protection Agency to enforce the CCPA alongside the attorney general and further provides a limited private right of action. Specifically, California's private right of action is limited to data breaches where a consumer's nonencrypted and nonredacted personal information is subject to unauthorized access and exfiltration that is caused by a business's violation of the duty to implement and maintain reasonable security procedures and practices. While many of these state laws were passed with "cure" periods, which allow organizations to cure alleged violations of the law within a specified period, around half of these cure periods expire after the first year of the law's enforceability, or in the case of California, have expired.

B. Developments in the Consumer Data Ecosystem, Data Brokers in the Spotlight

Regulatory concern and political commentary about the data broker business in the U.S. is not new. Over the past decade, Congress has continued to show interest in the data broker industry, the FTC has called for greater transparency and accountability from over the past several years, and several states have become active in this area. This interest continued in 2023.

Consumer Financial Protection Bureau (CFPB) proposed rulemaking

The CFPB started issuing rules on several topics affecting the consumer data ecosystem, as outlined in its plans for rulemaking under the FCRA. The proposed rulemaking will significantly impact data brokers, data aggregators, consumer reporting agencies (CRAs), furnishers of data to CRAs, sources of data for data brokers and data aggregators, and end users of data. CFPB Director Rohit Chopra highlighted one aspect of the proposal: a rule barring the reporting of medical debt collections through the credit reporting system, aiming to prevent medical debt collectors from exploiting the credit reporting system to pressure patients into paying bills they may not owe.

The proposed rulemaking could potentially reach many businesses and use cases that do not currently meet the FCRA's definition of CRA or consumer report under existing FCRA Regulation V. The CFPB's outline suggests that "credit header" data (generally, identifying information that does not relate to creditworthiness), used for decades to prevent fraud and identity theft, will no longer be permitted for those use cases outside the limited set of FCRA "permissible purposes" or under the CFPB's new proposed strict rules for obtaining consumer consent. This change would be just one of the many significant shifts by the CFPB from how the industry and courts have understood the FCRA over the past 50 years.

The proposed rulemaking will affect participants in the consumer data ecosystem in many ways. For instance, data brokers and data aggregators would only be able to sell data for permissible purposes allowed by the FCRA. Furnishers would have to investigate and respond to legal disputes or disputes on a "systemic" basis, although the CFPB has not yet provided details on how to define these terms. The proposed rulemaking also contemplates excluding any collection or distribution of medical debt collection information altogether by CRAs and would prohibit end users from considering such information.

The CFPB's proposed rule is expected to face significant legal challenges due to its sweeping reform of the FCRA's scope and obligations. If the CFPB's proposed rulemaking proceeds as outlined, it will complement other privacy and data security efforts led by the FTC and other agencies and have a dramatic effect across the board for all businesses involved in the consumer data ecosystem. A draft of the proposed rules is expected to be released for public comment later in 2024, but a final rule is unlikely for at least a year or more.

FTC and congressional signals

In the spring, the U.S. House of Representatives' Energy and Commerce Subcommittee held a hearing to examine the role of data brokers in the digital economy and the potential exposure of private and sensitive consumer information. The FTC has consistently demonstrated skepticism if not antipathy for the data broker industry, which was not absent this year. In his remarks at a fall 2023 data summit, the FTC's consumer protection head, Sam Levine, called out the data collection practices of data brokers as "posing serious threats to the constitutional liberties of Americans." In 2022, the FTC filed a lawsuit (ultimately unsuccessful) against data broker Kochava, alleging that the company sold sensitive location data that could endanger consumers, but Levine's comments may indicate that the federal focus on data brokers will only continue.

Changing the state data broker game

While data brokers are poorly understood but widely criticized organizations, they have come under increased criticism at the state level in recent years. Vermont and California have had data broker registration laws since 2018 and 2019, respectively, and in 2023, California significantly amended its data broker law when it passed the Delete Act. The Delete Act imposes additional disclosure and registration requirements on data brokers and moved enforcement of the data broker registry to the state's privacy regulator, the California Privacy Protection Agency (CPPA). The Delete Act will require data brokers to support deletion requests though a central "deletion mechanism" to be developed and administered by the CPPA, creating a central mechanism through which consumers could address all California data brokers with a single request. Finally, Oregon and Texas passed new data broker laws in 2023: H.B. 2052, which requires data brokers to register with the state of Oregon as of January 1, 2024, and S.B. 2105, which came into effect on September 1, 2023, and requires data brokers to register with the Texas Secretary of State.

C. New Restrictions and Liability for Online Advertising

The seven new state privacy laws passed in 2023 require applicable businesses to provide consumers with an opt-out for the use of their

personal information for certain types of targeted advertising. Colorado, Connecticut, Delaware, Montana, Texas, and California have gone further and require businesses to recognize universal opt-out mechanisms. Universal opt-out mechanisms, such as the global privacy control (GPC), are technical signals that are broadcast from consumer browsers or browser extensions that must be treated by the recipient site as opt-outs from the sale and/or sharing of their personal information. This requirement signals a shifting of the burden to exercise privacy rights from individuals to businesses. California currently requires businesses to recognize the GPC under the CCPA as reflected in its 2022 enforcement action against Sephora, though it has not given more specific guidance on what constitutes a universal opt-out mechanism. The Colorado Attorney General has published a short list of acceptable universal opt-out mechanisms that it will consider as binding under the Colorado Privacy Act (CPA). Companies doing business in Colorado were required to comply with consumer requests submitted through a universal opt-out mechanism as of July 1, 2023. Companies doing business in Colorado and Montana will need to comply with opt-out rights by July 1, 2024, and companies doing business in Texas and Delaware must comply by October 1, 2024, and January 1, 2025, respectively.

AdTech has also been top of mind for federal regulators. The FTC and the Department of Health and Human Services issued a joint letter to hospital systems and telehealth providers on the privacy and security risks from online tracking technologies. The letter jointly reminded entities subject to the Health Information Portability Accountability Act (HIPAA) that they are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of protected health information to third parties.

Looking ahead to 2024, the right to opt out of profiling may take center stage, as California will likely issue regulations under the CCPA addressing automated decision-making, which will include whether companies must offer an opt-out for all "profiling" involving advertising or whether an opt-out is only required when the profiling results in a legal or similar effect. Other states have generally only required an opt-out when profiling results in a legal or similarly significant effect; however, California's draft regulations, which were published in December, include an option for requiring an opt-out for all profiling involved in "behavioral advertising." This could have broad impact on advertising if the opt-out is required for activities that don't fall under the current CCPA definition of "cross-contextual behavioral advertising." For example, if an opt-out were required for profiling involving only first-party data, this would greatly expand opt-out rights and obligations. This is an area to watch in 2024 as California continues the process of developing final regulations for these important topics.

D. Children's Privacy

2023 brought an increased focus on children's privacy and online safety at the state and federal levels.

State activity

Connecticut, inspired by California's Age-Appropriate Design Code (CAADC), amended its comprehensive privacy law to prohibit certain processing as it pertains to children. On July 1, 2024, the CAADC will be applicable to organizations that develop and provide an "online service, product or feature" that is "likely to be accessed" by consumers who are under the age of 18, going far beyond the federal Children's Online Privacy Protection Act (COPPA) in both reach and potential applicability.

Importantly, the CAADC requires organizations to conduct privacy impact assessments that specifically identify how the online service uses children's personal information, identify potential risks of the proposed uses, and specify a plan to mitigate any identified risks, underscoring the importance for organizations to ensure that their privacy risk assessment process is revised to address CAADC requirements, where applicable. While the CAADC continues to be controversial (and is still subject to legal challenges), other states have

continued to adopt privacy-adjacent laws to protect children, such as the spate of laws regulating the use of social media by children passed in Arkansas, Florida, Louisiana, Utah, and Texas.

Further demonstrating the close relationship between concern for online trust and safety, especially for children and other at-risk populations, the attorneys general (AGs) of 54 states and territories called on Congress to address bad actors who generate child sexual abuse material (CSAM) using AI. The AGs asked Congress to establish an expert commission to study how AI can be used to generate CSAM, with a specific request for the commission to operate on an ongoing basis.

Federal activity

The FTC undertook several COPPA-related enforcement actions, proposed amending the COPPA Rule, and filed an amicus brief arguing that state-level legislation that proscribes the same conduct forbidden by COPPA is not preempted. The FTC's notice of proposed rulemaking seeks to significantly modernize and expand the reach of the COPPA in ways that reflect aspects of the FTC's enforcement activity earlier in the year. Specifically, the FTC's proposed revisions would restrict the use of persistent identifiers and push notifications to children, require separate parental consent for targeted advertising, impose new limitations on the ways that education technology providers would be permitted to use students' data, clarify COPPA's existing data minimization requirements, and strengthen the programmatic security requirements for organizations processing children's data.

The FTC COPPA enforcement efforts in 2023 involving children's data included a compliance order and $6 million settlement with Edmodo, an education technology provider, for collecting personal data from children without obtaining parental consent, using that data for advertising purposes in violation of COPPA, and for unlawfully outsourcing its COPPA compliance responsibilities to schools; and a $20 million settlement with Microsoft over allegations that the company violated COPPA by improperly collecting and retaining personal information from children through its Xbox gaming consoles and Xbox Live online services.

Finally, perhaps boosting the momentum gathering behind the passage of state laws aimed at protecting children's privacy, the FTC filed an amicus brief in the Ninth Circuit case *Jones v. Google*, asserting its support for the court's position that COPPA only preempts state law claims that are "inconsistent" with COPPA's treatment of regulated activities. Considering this decision, companies processing children's data should prepare for an increase in state law based private causes of action and enforcement actions.

E. Artificial Intelligence

2023 saw dizzying legislative activity across the globe — from broad regulation emerging in the European Union to the adoption of narrowly targeted municipal and state laws in the United States aimed at certain industry sectors. From the EU's act on artificial intelligence to the issuance of a sweeping executive order from the Biden administration and the publication of many position papers and statements from global regulators – we see consensus around the need to regulate AI but no convergence around precisely how AI should be governed or by whom.

EU AI Act

In the final month of 2023, after more than two years following the first draft of the EU AI Act, the European Union announced agreement on a comprehensive horizontal law regulating AI. The AI Act establishes risk-based obligations for providers and users of AI; with some exceptions, certain uses of AI will be barred as presenting unacceptable levels of risk (such as social scoring and real-time facial recognition). High-risk systems that negatively affect the safety or fundamental rights of people will be regulated under existing safety legislation (such as cars and medical devices), and others will need to be registered in an EU database (such as law enforcement and employment-related uses). Finally, general-purpose and generative AI must comply with transparency requirements, while limited-risk AI systems need only meet minimal transparency requirements that leave more discretion to the end

users of the products as to whether and how to engage with them. The AI Act, once its technical terms are finalized, will, like the EU GDPR, have extraterritorial effects and apply to any organization that is offering AI systems or services in the EU.

Tension between privacy laws and AI innovation

While the EU AI Act will initially live in parallel with the GDPR, it is also grappling with the fact that specific requirements imposed on organizations by the GDPR may hinder innovation in the development of AI tools and systems. Time will tell if the tension between these two pieces of legislation will lead to adjustments to one or both.

For example, the Confederation of European Data Protection Organization published a paper grappling with some of the challenges for AI developers when dealing with the nature of AI and the limitations of the GDPR, for several reasons, but primarily due to the tension between the GDPR's objective of protecting personal information, and the reality that AI systems are trained on massive amounts of data, which inherently, due to its broad definition, will include some personal data for which it would be in many cases extremely difficult, if not impossible, for an AI developer to have a clear legal basis for processing.

At the same time, the G7 data protection and privacy authorities, regulators from the U.S., France, Germany, Italy, Canada, Japan, and the United Kingdom issued a joint statement on the recent developments and challenges of generative AI technologies from a data protection and privacy perspective. The statement highlighted several areas of concern regarding privacy and data protection risks in the context of generative AI tools, including the legal authority for processing personal information, particularly for minors and children; security safeguards against threats and attacks; and measures to ensure the accuracy and non-discriminatory nature of personal information generated by AI tools. The statement stressed the importance of accountability and data minimization while emphasizing the need for transparency, technical documentation, and measures to ensure individuals can exercise their rights in relation to generative AI tools. Practically, the statement reminded organizations working on generative AI initiatives to comply with existing laws and to adhere to well-established data protection principles such as "Privacy by Design" in the design, conception, operation, and management of new products and services that use generative AI, and to document these choices in a privacy impact assessment.

U.S. regulatory agencies emphasize the applicability of existing laws to govern AI

The FTC, Department of Justice (DOJ), CFPB, and Equal Employment Opportunity Commission (EEOC) released the "Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems." The statement emphasized that existing

law applies to the use of automated systems just as it applies to other practices and that the regulators intend to enforce laws regarding civil rights, non-discrimination, fair competition, and consumer protection regardless of a violator's use of AI. The statement strongly indicates continued regulatory focus on the potential of AI systems to produce discriminatory outcomes as a result of biased and nonrepresentative datasets, opaque and private models, and the ability of AI models to be used to harm or disadvantage individuals or society more broadly.

Except for the DOJ, each of the agencies has been independently acting in the AI space, lending credence to their words. For example, the CFPB issued guidance regarding credit denials by lenders using AI. The FTC approved an omnibus resolution authorizing the use of compulsory process in its nonpublic investigations involving AI-related products and services, streamlining the FTC's ability to issue civil investigative demands in such investigations and perhaps signaling an increased enforcement focus on AI-related products. Finally, the EEOC released AI guidance for employers reiterating that its Uniform Guidelines on Employee Selection Procedures apply equally when AI is used to make decisions regarding hiring, retention, promotion, or similar actions.

NIST releases new AI Risk Management Framework

In the vein of using existing resources and encouraging responsible AI governance practices, the National Institute of Standards and Technology (NIST), part of the Department of Commerce (DOC), released the AI Risk Management Framework (AI RMF) – a nonbinding guide for organizations to support the responsible and secure design, development, use, and evaluation of AI products, services, and systems. Formed through months of collaboration with public and private sector stakeholders, the AI RMF articulates characteristics of trustworthy AI systems — notably, that systems should be "privacy-enhanced." This refers to the use of privacy-enhancing technologies and other measures to help safeguard user information. The DOC also launched the Public Working Group on Generative AI to assist NIST develop further organization-focused guidance on AI-related risks. In 2024, we expect NIST to continue to push public-private collaboration to ensure AI innovation proceeds with minimum risk.

State and local lawmakers take AI matters into their own hands

In addition to congressional and federal agency activity, state and municipal agencies have not hesitated to move forward in the absence of comprehensive legislation or guidance. For example, the Colorado Division of Insurance (DOI) issued a draft of proposed regulations related to algorithm and predictive model governance. The regulations would require life insurance companies that use external consumer data and information sources (ECDIS), as well as algorithms and predictive models using ECDIS, to establish a governance and risk management framework that ensures the ECDIS are credible in all material respects, and that their use in any insurance practice does not result in unfair discrimination. The framework proposed by Colorado's DOI includes elements that mirror other efforts to regulate AI and force accountability for their models and impact.

Further, the New York City Department of Consumer and Worker Protection (DCWP) adopted final rules to implement the city's Local Law 144 prohibiting employers and employment agencies from using any AI tool in the hiring process unless that tool has undergone a bias audit to comply with requirements to report on impacts on race, ethnicity, and sex to the EEOC. The rules also clarified examples of where a bias audit may be required and added requirements for published results of bias audits as well as the furnishing of specific notices to employees or job candidates.

Other municipalities, such as Seattle, San Jose, and Santa Cruz County, have also been active in AI governance. Santa Cruz County initiated development of policies related to the use of AI in county operations, and its board of supervisors adopted an Artificial Intelligence Appropriate Use Policy three months later. The county planned to monitor usage over six months, collect feedback, and issue updates to the policy in accordance with board direction, before reporting back to the

board in early 2024. San Jose released its first set of employee guidelines for generative AI, which included guidelines for the use of direct services like ChatGPT and extensions like Compose.ai when conducting work on behalf of the city. Seattle released a Generative Artificial Intelligence Policy to align with priorities outlined in President Biden's AI executive order from November. The purpose of the policy is to set forth requirements for city departments, including vendors, contractors, and volunteers who operate on behalf of the city, to observe when acquiring and using software that meets the definition of "generative artificial intelligence."

While some state and municipal agencies are creating research groups and drafting policies that govern, but allow for, the use of AI in government functions, Maine Information Technology took a different approach when it issued a complete moratorium on the use of generative AI on any device connected to the state's network for at least six months. The directive prohibits all executive branch state agencies from adopting or using generative AI technology for all state business or on any device connected to the state's network. The temporary ban is intended to give the state time to research and evaluate risks posed by AI technology, including threats of misinformation, bias, privacy, and cybersecurity challenges.

Congressional activity on AI

In 2023, regulators continued to gather information on how to regulate AI in a way that will balance innovation with consumer safety and social justice but fell short of proposing concrete legislation. For example, the Senate Judiciary Committee's Subcommittee on Privacy, Technology held hearings to discuss issues involving AI. The hearings observed the potential benefits of AI while acknowledging the need for transparency and accountability to address ethical concerns, protect constitutional rights, and prevent the spread of misinformation. The committee has since urged lawmakers to move ahead with AI legislation. Congress also conducted a widely covered AI Insight Forum with tech leaders who pledged fidelity to responsible AI development, but which was otherwise short on regulatory requirements or binding commitments from industry. Looking ahead to 2024, regulators will presumably shift from information gathering to passing comprehensive AI legislation. There is significant incentive to do so expediently, given the threats posed by AI and also the fractured landscape that is emerging at the state and local level as well as through the ongoing regulatory enforcement of existing laws.

Executive order addressing AI

In the aftermath of much congressional and state-level activity on AI, President Biden signed the most comprehensive executive order (EO) on AI to date, outlining directives to manage AI risk and development. The EO reflects the administration's aim to enhance AI security, establish U.S. leadership in global AI policy, and respond to increasing AI competition, particularly from the EU, UK, and China. Notably, the EO imposes various requirements to safeguard national security, including national economic security, or national public health and safety. Given that AI systems can be vulnerable to manipulation, developers must notify the federal government when formulating an AI foundation model that poses a serious risk to national security and share the results of all safety tests. It further directs the NIST to develop a framework for red team testing of AI systems that the Department of Homeland Security and the Department of Energy will utilize in their regulation of critical infrastructure sectors.

Notification at the developmental stage proactively addresses the inability of many AI models to "forget" information once functional, as well as questions concerning creators' ability to control a system as it becomes increasingly "intelligent." The interpretation of many of the terms in the EO, including definitions of "national security" and "public health and safety" will come from federal agencies charged with clarifying these provisions within their respective spheres. For example, the Department of Health and Human Services released a 916-page rule that regulates AI algorithm transparency and information sharing for health care providers. Other agencies will likely soon follow suit. Regardless, companies developing AI systems must proceed cautiously and only after conducting due diligence, considering these mandates.

The EO also sets parameters for AI implementation within federal agencies, focusing on risk minimization and noting substantive areas of concern. For example, it directs the FCC to research and provide support to next-generation technologies that incorporate AI, such as 6G, to increase network security and interoperability. It further expounds upon the areas of AI procurement, hiring of AI professionals, and training of current federal employees in AI-relevant fields for all federal agencies.

There is widespread concern in many job sectors that AI will potentially displace certain workers as a more efficient, less costly alternative to human labor. To address this concern, the EO directs the development of best practices to mitigate AI-related labor harm such as job displacement, workplace health and safety, and AI surveillance of workers. The EO also commissions a study of the potential AI impact on labor markets, including how the federal government can support AI-disrupted workers.

The EO also recognizes that AI carries with it profound privacy implications for consumers, particularly within its data collection and retention functions, and recommends funding for research into technologies like cryptographic tools through the creation of a research coordination network to advance privacy-based technology development. The National Science Foundation will also work with the network to promote these technologies within federal agencies.

While the EO is an encouraging first step in signaling a flexible and multi-disciplinary approach to AI regulation, the broader federal government's commentary and regulatory oversight of AI are still nascent. The reality is that neither local nor global authorities are waiting for U.S. national leadership to act, so it very much remains to be seen whether and how the administration, Congress, and federal agencies will act, and whether the U.S. will be able to lead in a way that preserves innovation and provides incentives for global companies to key their compliance programs to U.S. frameworks or to principally align with other global frameworks that emerge first.

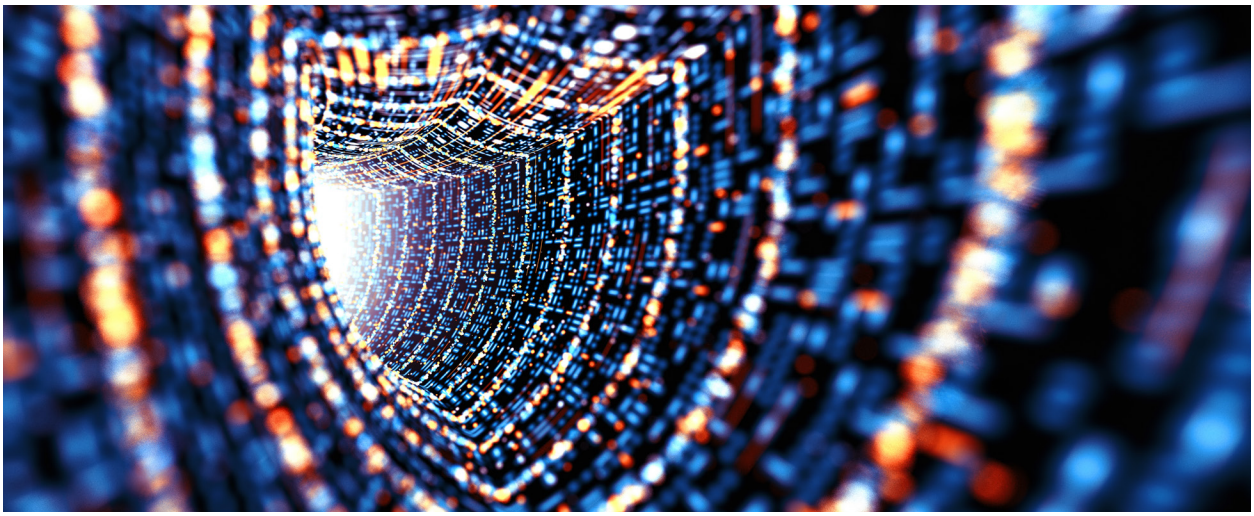
F. Notable Cyber-Related Policy Developments and Administrative Activity

National defense capability

In 2023, the U.S. took several significant steps to better organize its national defense capabilities in response to the growing threat of cyber-enabled weapons and coordinated attacks. Of the notable accomplishments, the DOJ published a comprehensive cyber review documenting the cyber capabilities of hostile nations, including China, Russia, Iran, and North Korea, and their escalating use of cyber-enabled tools to engage in a spectrum of activities that pose grave threats to national security. The cyber review cited threats ranging from stealing sensitive technologies and conducting cyber intrusions to suppression of free information flow to risks to critical infrastructure. Acting in response to the cyber review and to further enable the national cybersecurity strategy released by the White House in the spring, a new national security cyber section (NatSec Cyber) was created within the DOJ's National Security Division to better situate the U.S. to respond to nation-state threat actors and state-sponsored and other cyber-enabled threats to the nation's security. NatSec Cyber will operationalize a more intentional and coordinated approach to cyber defense, forging better interagency partnerships, collaborating with global allies, engaging in more public-private partnerships, and leveraging the power of federal law enforcement tools with the intent of enabling the U.S. to have a cohesive and agile response to evolving cyber threats.

FCC launches Privacy and Data Protection Task Force

The FCC also acted in 2023 to implement measures designed to better protect the U.S. telecommunications ecosystem from data breaches and supply chain vulnerabilities, particularly among the third-party entities servicing the communications providers that the agency regulates. Specifically, the FCC created a privacy and data protection task force to assess and coordinate the privacy and data protection needs for rulemaking, enforcement,



and public awareness across the FCC. In its first working meeting, the task force announced that its "top priority" would be to protect the privacy of consumer information by ensuring that those in the regulated communications sector adhere to the agency's privacy and data protection regulations.

New SEC cybersecurity disclosure rules for public companies

In 2023, the SEC adopted new rules requiring public companies and foreign issuers to disclose material cybersecurity incidents and provide annual reports on their cybersecurity risk management, strategy, and governance. The rules aim to ensure that companies disclose information about their cybersecurity governance and material impacts on their businesses in a consistent, comparable, and decision-useful way.

Under the rules, companies must disclose any material cybersecurity incident on the new Item 1.05 of Form 8-K within four business days after determining the materiality of an incident unless the company requests and the U.S. attorney general determines that immediate disclosure would pose a substantial risk to national security or public safety. The disclosure should describe the incident's nature, scope, and timing, as well as its material impact or reasonably likely material impact on the company. However, Form 8-K disclosures do not need to disclose specific or technical information about a planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident.

The rules also introduce Regulation S-K Item 106, requiring companies to describe their processes for assessing, identifying, and managing material risks from cybersecurity threats. This includes the material effects or reasonably likely material effects of risks from cybersecurity threats and previous incidents. Companies must also describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing these risks. These disclosures will be required annually on Form 10-K.

Form 6-K, 8-K, 10-K, and 20-F disclosures went into effect in December 2023. Smaller reporting companies will have an additional 180 days before they must begin providing the Form 8-K disclosure.

Proposed SEC amendments to Regulation S-P

The SEC also proposed amendments to Regulation S-P aimed at bolstering the protection of customer information. The proposed changes would require broker-dealers, investment companies, registered investment advisers, and transfer agents to notify individuals affected by data breaches that could potentially expose them to a risk of identity theft or other harm. Regulation S-P currently mandates that such entities have written policies and procedures:

(1) for the protection of customer records and information (the "safeguards rule"); and (2) for the proper disposal of consumer report information (the "disposal rule"). The proposed amendments seek to modernize these requirements to address the increased use of technology and associated risks since the original adoption of Regulation S-P in 2000.

The proposed changes would require covered institutions to establish written policies and procedures for an incident response program to address unauthorized access to or use of customer information. Barring certain exceptions, these institutions would need to notify individuals whose sensitive customer information was or is reasonably likely to have been accessed or used without authorization. Covered institutions would need to provide this notification as soon as practicable, but no later than 30 days after the institution becomes aware of such an incident.

These changes, if adopted, would impose notification requirements under federal law similar to those imposed by state data breach notification laws, as well as heightened requirements under the existing safeguards and disposal rules.

G. Notable State AG Enforcement

State AGs have historically been at the forefront of regulating emerging technology. Their expertise with enforcing existing laws to shape the regulatory environment, their resources when banded together as a multistate entity, and their agility in responding to novel issues at a local level make them the vanguard regulatory body when it comes to consumer protection in the rapidly evolving technological landscape. As described in the three examples below, in 2023 state AGs used this power to further develop the regulatory consumer privacy landscape in two notable areas: AI and data breach investigation.

State AGs wield their power by clarifying legislation and regulation through enforcement activity. By leveraging significant real-world experience and detailed industry knowledge, state AGs essentially develop the law to bring about far-reaching changes. Additionally, state AGs are employing their growing influence to engage with federal regulators to shape privacy regulation at the national level.

In 2024, state AGs will continue to use existing laws in conjunction with new data privacy legislation to bring enforcement actions through multistate investigations and partnerships with other state and federal agencies. Violations of privacy and consumer protection regulations carry significant financial and reputational risk. Companies should pay close attention to new legislation, guidance, and related enforcement activity by state AGs to prepare for substantial changes on the horizon.

New York AG scrutinizes Madison Square Garden facial recognition technology

In January 2023, New York Attorney General (AG) Letitia James scrutinized Madison Square Garden Entertainment Corporation (MSG) for its use of facial recognition technology. MSG's technology, implemented in 2018 for security purposes, is being used controversially to identify and block attorneys involved in litigation against MSG, impacting around 90 law firms. This practice is contentious due to New York's biometric identifier law, necessitating full disclosure of such usage to consumers.

Concerns raised by James focus on the reliability of facial recognition technology and its potential for discrimination. MSG was asked to justify its policy and demonstrate compliance with relevant federal, state, and local human rights laws. While MSG argues this strategy prevents attorneys from gathering incriminating evidence, James countered that it could deter attorneys from representing legitimate cases against MSG.

As MSG faces lawsuits from barred attorneys claiming civil rights violations, this case highlights the growing regulatory scrutiny of biometric privacy. Lawmakers and regulators are developing policies and legislation to protect consumer biometric data, indicating a rise in regulatory attention towards companies using facial recognition technology. Businesses must reassess their privacy policies and ensure compliance with biometric laws, considering the legal and ethical implications of such technology.

AGs require company to protect user data on ovulation tracking app

On May 17, District of Columbia Attorney General Brian Schwalb announced a settlement with Easy Healthcare Corporation relating to its ovulation tracking app, "Premom." Easy Healthcare provides several home health care products, including Premom — an ovulation tracker, menstrual tracker, and fertility tool. However, the International Digital Accountability Council raised concerns in 2020 that the app was unknowingly sharing sensitive user data with third parties, including two China-based companies known for contentious privacy practices.

A coordinated investigation by the District of Columbia, Oregon, Connecticut, and the FTC confirmed the unauthorized data sharing. As part of the settlement, the company agreed to a $100,000 penalty to the states and significant changes to its privacy practices to better protect sensitive reproductive data of consumers. The changes include limiting data collection to necessary, specified purposes, enhancing consumer disclosures, prohibiting data sharing without consent, and allowing users to request deletion of their information. The company is also implementing a vendor risk management program and will undergo third-party assessments of its data security and privacy practices.

This case underscores the importance for companies to regularly audit their privacy practices, particularly if their products and services, including mobile apps, collect consumer data. Accurate disclosures reflecting the business's information practices, including data collection and sharing, are critical to avoid regulatory scrutiny and potential penalties. Failure to ensure such transparency could lead to substantial regulatory investigations, highlighting the need for companies to be proactive in ensuring their data practices comply with consumer privacy laws and best practices.

NY Attorney General reaches a $200K settlement with a law firm over a data breach

On March 27, New York Attorney General Letitia James announced a $200,000 settlement with New York City law firm Heidell Pittoni Murphy & Bach LLP (HPMB) following a 2021 data breach. The breach compromised the electronic protected health information (ePHI) and additional information of roughly 61,438 New York residents, including data such as birth dates, Social Security numbers, and medical history. An exploit in HPMB's email server allowed an attacker to access company systems in November 2021; despite being aware of the vulnerabilities and receiving patches from the software provider in April and May 2021, HPMB did not promptly apply these patches, leading to a large-scale data exfiltration in December.

James alleged HPMB violated multiple state and federal laws concerning data security and unauthorized acquisition of private information, including New York State Executive Law § 63(12), General Business Law (GBL) §§ 899-aa and 899-bb, and various provisions under HIPAA. James emphasized HPMB's failure to uphold reasonable practices to protect consumer information, such as regular risk assessments, data encryption, and data minimization practices. Additionally, James found HPMB in violation of GBL § 899-aa for not providing timely notification of the breach.

As part of the settlement, HPMB committed to maintain a comprehensive information security program aimed at protecting ePHI and other private information. This includes measures like encryption, network activity monitoring, penetration testing, implementing a patch management system, limiting data collection to necessary extents, and timely data deletion. The firm is also mandated to obtain a thorough information security assessment by a third party within one year, and again within the next five years. Affected consumers were offered two years of credit monitoring and identity theft services. This case underscores the increasing regulatory scrutiny concerning data security, emphasizing the need for businesses to prioritize robust measures for data protection.

H. Privacy Litigation

Developments in AdTech litigation

AdTech litigation runs the gamut and generally refers to legal disputes arising from the use of AdTech on websites. AdTech includes tools like session replay technology, chatbots, pixels, tags, and web beacons, which companies use to understand user interactions with their websites and to target or retarget consumers on third-party platforms like social media.

In 2023, companies that utilize AdTech were the target of litigations arising from the Video Privacy Protection Act (VPPA) and state wiretapping laws. In addition, AdTech companies were the subject of lawsuits arising from the misuse of OpenAI and ChatGPT.

VPPA litigation

AdTech lawsuits arise from technology associated with consumer interactions with websites. These lawsuits involved claims asserted under the VPPA and state wiretapping laws. The VPPA prohibits the disclosure of the identity of an individual and that individual's video-watching history without consent. Enacted in 1988 in response to a newspaper's publication of Judge Robert Bork's video-watching history during his Supreme Court nomination, the VPPA was intended to maintain the privacy of the videos that an individual rents from a brick-and-mortar video store. With the advent of technology and extinction of video rental stores, the VPPA is now being used to target companies that host videos on their websites and utilize pixel technologies to track and share video-watching information with Facebook for targeted advertising. The lawsuits have been bought against digital news providers, every major sports league, video streaming services, and retail entities that offer video content on their websites. Because the VPPA provides for statutory damages of the greater of $2,500 or actual damages and a violation of the statute alone has been found to establish standing, it has been a cause of action that has been asserted in hundreds of putative class actions.

In 2023, VPPA class actions took a hit with approximately 17 cases being dismissed. Courts in those cases found: (1) the VPPA does not apply to retailers who are not primarily engaged in the business of selling or renting audiovisual materials; (2) a subscriber to a newsletter who receives no additional benefits from the subscription is not a consumer within the meaning of the VPPA and cannot pursue a claim; and (3) where a URL is transmitted to a third party that does not disclose whether a video is watched, there is no basis for a VPPA claim. A summary of the cases supporting these principles is below.

In *Carroll v. General Mills, Inc.*, a district court recognized that businesses that are not primarily engaged in renting and selling videos are not subject to a VPPA claim because they are not a videotape service provider under the statute. In *General Mills*, a plaintiff consumer filed a putative class action against General Mills alleging the company violated the VPPA. *Carroll v. Gen. Mills, Inc.*, No. CV 23-1746 DSF (MRWx), 2023 U.S. Dist. LEXIS 155621, at *1 (C.D. Cal. Sept. 1, 2023). In support of his claim, plaintiff alleged he purchased General Mills' products, downloaded the General Mills app, and watched a video on baking on General Mills' website. *Id.* at *2. In response to a motion to dismiss, the court found that the VPPA claim failed because plaintiff could not plausibly allege that General Mills was a "video tape service provider" subject to the VPPA. The court noted that the VPPA claim failed because General Mills is "a company manufacturing and selling cereals, yogurts, cake mixes, dog food, and other products" and is not engaged in the business of delivering audiovisual material. *Id.* at *9. The court also noted, in response to plaintiff's contention that General Mills' website contains videos that the company profits from, that the allegations do not demonstrate General Mills is a videotape service provider because the videos are for brand awareness and there is no indication that General Mills profits off the videos themselves. *Id.* at *9-10. Other courts have reached a similar conclusion. *See, e.g.*, *Cantu v. Tapestry, Inc.*, No. 22-cv-1974-BAS-DDL, 2023 U.S. Dist. LEXIS 118474, at *25 (S.D. Cal. July 10, 2023) (dismissing VPPA claim because the complaint failed to plausibly allege a luxury fashion retailer is a "video tape service provider"). In *Carter v. Scripps Networks, LLC*, the plaintiffs alleged they subscribed

to the defendant's newsletter and watched video material on the defendant's website and therefore were "subscribers" capable of pursuing claims under the VPPA. No. 22-CV-2031 (PKC), 2023 WL 3061858, at *1 (S.D.N.Y. Apr. 24, 2023). Because the plaintiffs did not allege that their "status as newsletter subscribers was a condition to accessing the site's videos, or that it enhanced or in any way affected their viewing experience, they were not subscribers capable of pursuing a VPPA claim."

Other courts dismissed VPPA claims in 2023 where a plaintiff failed to allege a subscription enhanced or in any way impacted his/her video viewing experience. *See, e.g., Jefferson v. Healthline Media, Inc.*, No. 3:22-CV-05059-JD, 2023 U.S. Dist. LEXIS 91174, 2023 WL 3668522, at *3 (N.D. Cal. May 24, 2023) (dismissing VPPA claim where plaintiff failed to allege she received any kind of publication, let alone any good or service, in exchange for signing up for Healthline's email list; she could not establish she is a consumer for purposes of pursuing a claim); *Lamb v. Forbes Media LLC*, No. 22-cv-06319- ALC, 2023 U.S. Dist. LEXIS 175909, at *37 (S.D.N.Y. Sept. 28, 2023) (dismissing VPPA claim where plaintiff failed to allege he received anything of value in exchange for a Forbes login); *Gardener v. MeTV*, No. 22-cv-05963, 2023 U.S. Dist. LEXIS 115810, 2023 WL 4365901, at *4 (N.D. Ill. July 6, 2023) (finding that the plaintiffs were not subscribers under the VPPA because the plaintiffs' subscription to a newsletter was "unconnected to their ability to access video content" that was otherwise available on the website); *Salazar v. Paramount Glob.*, No. 3:22-cv-00756, 2023 U.S. Dist. LEXIS 123413, at *28 (M.D. Tenn. July 18, 2023) (plaintiff who signed up for a newsletter was not a subscriber capable of bringing a VPPA claim); *Salazar v. NBA*, No. 1: 22-cv-07935 (JLR), 2023 U.S. Dist. LEXIS 137982, at *9-10 (S.D.N.Y. Aug. 7, 2023) ("the Court does not find that Plaintiff's subscription to Defendant's newsletter rendered him a consumer of goods or services from a video tape service provider under the VPPA"); *Alex v. NFL Enters. LLC*, No. 1:22-cv-09239 (ALC), 2023 U.S. Dist. LEXIS 172991, at *9 (S.D.N.Y. Sept. 27, 2023) (dismissing VPPA claim because plaintiffs did not pay to subscribe to defendants' newsletters, nor did they "evince [a] desire to forge ties with" defendants when accessing free content on the team websites).

In *Martin v. Meredith*, a plaintiff sued the owner of People.com claiming it violated the VPPA by knowingly disclosing the video-viewing activities of website visitors without their consent through use of the social media platform pixel. 657 F. Supp. 3d 277, 281 (S.D.N.Y. 2023). In response to a motion to dismiss, the court found that the plaintiff failed to state a cognizable claim for a VPPA violation because the settings on the pixel used by www.people.com only enabled a user's social media ID and the webpage the user accessed to be transmitted. *Id.* at 283. The court found that "merely disclosing the name of the webpage a user visits does not indicate that the website visitor requested or obtained specific video materials from that webpage" even if the webpage contains a video.

Id. at 284. Accordingly, because plaintiff failed to allege any video-viewing information was transmitted to a third party, the VPPA claim was dismissed. *Id.* at 285.

Other courts have considered arguments similar to those asserted in *Martin* and denied motions to dismiss, finding whether a URL sufficiently identifies video-viewing information is an issue of fact that should not be resolved on a motion to dismiss. *See Harris v. Pub. Broad. Serv.*, No. 1:22-CV-2456-MLB, 2023 U.S. Dist. LEXIS 45888, 2023 WL 2583118, at *6 (N.D. Ga. Mar. 20, 2023); *Ghanaat v. Numerade Labs, Inc.*, No. 4:23-cv-00833-YGR, 2023 U.S. Dist. LEXIS 157378, at *11 (N.D. Cal. Aug. 28, 2023).

CCPA litigation

There were numerous developments in CCPA litigation as courts grappled with the scope of the statute's language and its amended provisions under the California Privacy Rights Act (CPRA). The CCPA limits its private right of action to "consumer[s] whose nonencrypted and nonredacted personal information…is subject to an unauthorized access ***and*** exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Cal. Civ. Code § 1798.150(a). The CCPA's limited private right of action likewise narrows the scope of litigation, as reflected by the 2023 cases discussed below.

Scope of Private Right of Action

Courts continued to limit the scope of private right of actions and explained what is needed to state a plausible CCPA claim.

In *Tate v. EyeMed Vision Care, LLC*, No. 1:21-CV-36, 2023 WL 6383467, at *10 (S.D. Ohio Sept. 29, 2023), a plaintiff alleged that a defendant violated Cal. Civ. Code § 1798.100(e) by failing to implement reasonable security measures to protect its customers' personal information from unauthorized access. The court made short work of the CCPA claim asserted against EyeMed Vision because, under Cal. Civ. Code § 1798.145(c)(1)(A), a covered entity like EyeMed, which is subject to HIPAA, is exempt from CCPA liability. In making this ruling, the court rejected the plaintiff's argument that § 1798.145(c) only exempts a covered entity with regard to the exposure of personal health information and not with regard to personal information. The court found § 1798.145(c)(1)(B) exempts health care providers subject to HIPAA from the CCPA "to the extent the provider…maintains patient information in the same manner as medical information."

Courts have also been reluctant to dismiss CCPA claims at the pleadings stage. For example, in *Baker v. ParkMobile, LLC*, No. 1:21-CV-02182, 2023 WL 6536191, at *5 (N.D. Ga. Sept. 29, 2023), a defendant sought dismissal of the complaint on the basis that the information allegedly accessed either: (1) did not fit within the definition of "personal information" under the CCPA; or (2) was encrypted such that there was no unauthorized disclosure. The court found that the defendant's definition of "personal information" argument was an issue of fact that could not be resolved on a motion to dismiss. As for the second argument concerning encryption, the court found that the parties' briefing was insufficient for the court to rule as a matter of law that plaintiffs' claim failed on the encryption issue. The court acknowledged that the defendant relied on the substantive plain language of § 1798.150 while plaintiffs relied primarily on the definitional provision of § 1798.82(i)(4). However, the court denied the motion as it was "an issue of first impression," and felt it more appropriate to decide the issues after discovery occurred.

Notice-and-Cure Provision

Because the CCPA does not define what qualifies as a "cure," it is likely this will be a significant area of future CCPA litigation. Under the CCPA before the amendments under the CPRA, if a business "actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business." Cal. Civ. Code § 1798.150(b). The CPRA amended the cure provision, stating that "the implementation and maintenance of reasonable security procedures and practices…following a breach does not constitute a cure with respect to that breach." *Id.*

Two district court decisions in 2023 provide some guidance on the cure provision. In *Florence v. Ord. Express, Inc.*, the Northern District of Illinois denied a motion to dismiss and allowed the CCPA claim to proceed on the basis that (1) plaintiff sufficiently alleged that he sent a notice informing the defendant of its alleged violation and (2) the defendant's enhancement of its security measures was not a cure of the violation but merely implementation and maintenance of reasonable security procedures and practices. *Florence v. Ord. Express, Inc.*, No. 22 C 7210, 2023 WL 3602248, at *7 (N.D. Ill. May 23, 2023).

In *Guy v. Convergent Outsourcing, Inc.*, the Western District of Washington analyzed whether a failure to issue a pre-suit cure notice would result in a dismissal of the CCPA claim with prejudice. No. C22-1558 MJP, 2023 U.S. Dist. LEXIS 125332, at *28 (W.D. Wash. July 20, 2023). The court found that it did not, noting that a dismissal without prejudice accords with the remedial nature of the CCPA's notice provision and allows defendant the opportunity afforded to it under the CCPA to cure the injury.

Looking forward in 2024, parties will continue to challenge the contours of the CCPA's undefined or ambiguous terms, and courts will engage in statutory interpretation to provide guidance to litigants. Due to the amended language, courts will likely also weigh in on parties' disputes about whether the pre-CPRA version of the CCPA applies to the claims of a lawsuit and its impact on CCPA claims. It is critical for businesses to understand, assess, and implement best practices in the midst of this evolving regulatory and litigation regime.

Wiretapping litigation

In 2023, an increase in lawsuits alleged violations of the federal Wiretapping Act and other state wiretap and surveillance laws associated with website tracking technologies, including session replay and chatbots. The majority of the filings in 2023 asserted claims under the California Invasion of Privacy Act (CIPA) because of the ability to recover statutory damages and the language of the act, which holds that any communication occurring with a California resident requires two-party consent to be recorded or intercepted. Specifically, Section 631(a) of CIPA prohibits a third party from intercepting, reading, or attempting to read or learn the contents or meaning of "any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within [California]" without the consent of "all parties to the communication." Cal. Penal Code § 631(a).

A number of decisions under CIPA § 631(a) have focused on whether a tracking technology intercepted a communication in transit and simultaneously disseminated that communication to an unannounced third party. One defense that emerged was the party exception to a wiretapping claim. Under this exception, a party to a conversation cannot be liable for a CIPA violation for eavesdropping or tape recording its own conversation. *Javier v. Assur. IQ LLC*, No. 20-CV-02860-CRB, 2023 WL 3933070 (N.D. Cal. June 9, 2023) (recognizing a party to a conversation cannot be held liable as an eavesdropper); *Licea v. Cinmar, LLC*, 659 F. Supp. 3d 1096, 1102 (C.D. Cal. Mar. 7, 2023) ("Defendant was a party to the purported conversation with Plaintiffs and, as such, cannot be held liable" for a CIPA violation); *Esparza v. Lenox Corp.*, No. C 22-09004 WHA, 2023 WL 2541352, at *2 (N.D. Cal. Mar. 16, 2023) ("Because defendant is party to the communication in question, defendant's own recordation of the chat conversation cannot give rise to liability under Section 631(a).").

Relying on this principle, courts have recognized that a vendor who does not have the capability to use or divulge the contents of a communication to anyone other than the defendant is not a third party who intercepts a communication in violation of CIPA. For example, in *Swarts v. Home Depot, Inc.*, a plaintiff filed a putative class action alleging, among other things, that Home Depot violated CIPA by using LivePerson technology, which is a website live chat feature used to access and analyze recorded conversations to understand what customers want, to fix inefficiencies, and to increase sales. Home Depot moved to dismiss the CIPA claim on the basis that the plaintiff failed to allege that LivePerson or any other third party can use the information for any purpose other than relaying it to Home Depot. No.

23-cv-0995-JST, 2023 U.S. Dist. LEXIS 153477, at *19-20 (N.D. Cal. Aug. 30, 2023). The court agreed and dismissed the CIPA claim. It found the complaint failed to "allege that [the vendor], or any other third party, can use the information obtained for any other purpose besides relaying it to [the defendant]," and therefore there were no allegations of an interception of a conversation within the meaning of CIPA to state a cognizable claim. *Id.* at 21. In this regard, the court noted that the vendor was akin to a recorder for the defendant. *Id.*

Other courts made similar rulings in 2023. *See, e.g., Yockey v. Salesforce, Inc.*, No. 22-CV-09067-JST, 2023 U.S. Dist. LEXIS 150262, 2023 WL 5519323, at *5 (N.D. Cal. Aug. 25, 2023) (dismissing CIPA claim because allegations that live chat communications had been "routed" through a server controlled by a third party and that the vendor analyzed the communications in real time did not support a reasonable inference that the vendor has the capability of using the communications for any purpose other than furnishing them to the defendant); *Williams v. DDR Media, LLC*, No. 22-cv-03789-SI, 2023 U.S. Dist. LEXIS 145489, 2023 WL 5352896, at *4 (N.D. Cal. Aug. 18, 2023) (dismissing CIPA claim because the third party was more akin to a tape recorder vendor than to an eavesdropper).

Another issue involving CIPA claims was whether the statute requires a plaintiff to allege the "contents" of a communication to state a viable claim for a CIPA violation. Under CIPA and the federal Wiretapping Act, the contents of a communication to support an actionable interception include any information about the substance or meaning of a communication, but do not include "record information," such as the name, address, or subscriber information of a website user. *In re Zynga Privacy Litigation*, 750 F.3d 1098, 1106 (9th Cir. 2014).

The Central District of California in *Byars v. Goodyear Tire & Rubber Co.* addressed the obligation to plausibly allege the contents of a communication to assert a CIPA claim under § 631(a). 654 F. Supp. 3d 1020, 1024 (C.D.Ca. 2023). There, a plaintiff alleged Goodyear used a third-party vendor to embed code into its chat feature, which enabled Goodyear to record and transcribe her private conversations and the third party to intercept and eavesdrop on communications in the website chat feature. *Id.* Goodyear responded by moving to dismiss the Section 631(a) claim on the basis that plaintiff failed to allege the contents of any communication that was intercepted. In denying the motion to dismiss, the *Goodyear* court held there is no requirement under Section 631(a) of CIPA to allege "the exact contents of a communication" at the motion to dismiss stage; all that is required is to show "the contents were not record information, such as a name and address." 654 F. Supp. 3d 1020, 1027 (C.D. Ca. 2023). More specifically, the court found that by alleging she used the chat technology on Goodyear's website and the technology collected and shared sensitive personal information, the allegations in the complaint plausibly alleged more than mere record information. *Id.*

In addition to issuing a ruling on the pleading requirements under Section 631(a) of CIPA, the *Byars* decision is better known for its decision under CIPA Section 632.7, which highlights the conflict over how CIPA is interpreted. Under Section 632.7, a party is prohibited from intercepting a communication occurring between telephones. *Id.* at 1028. Goodyear moved to dismiss the Section 632.7 claim on the basis that plaintiff's communications with its website were not a communication between two telephones for purposes of a 632.7 claim. *Id.* The court disagreed and held "there is no requirement that Byars allege the type of telephonic device used by Goodyear" to state a claim under Section 632.7.

Two weeks after the *Goodyear* ruling, another Central District of California court, in *Byars v. Hot Topic, Inc.*, which involved the same plaintiff and identical allegations, dismissed the CIPA Section 632.7 and claim. The *Hot Topic* court acknowledged the *Goodyear* holding and disagreed with it, finding no basis for a Section 632.7 claim because "there is no possible basis to conclude" that plaintiff's attempts to broadly construe the term "landline telephone" included defendants' computer equipment. *Byars v. Hot Topic, Inc.*, 656 F. Supp. 3d 1051, 1070-71 (C.D. Cal. 2023).

This conflict, and the decisions that have allowed CIPA claims to survive motions to dismiss, will likely result in continued filings in 2024, which we hope will lead to more clarity on the scope of CIPA and what it prohibits.

Standing

Although many Article III standing arguments have been unsuccessful in privacy litigation, 2023 saw the courts' willingness to dismiss Wiretapping Act causes of action that are based on the use of session replay technology. This technology enables a website operator to know what a user did while on its website or app by capturing clicks, mouse movements, page scrolls, and URLs of webpages visited.

Courts faced with a Rule 12(b)(1) motion to dismiss involving privacy violations arising from the use of session replay technology have found no standing exists because the session replay technology did not capture personal information. For example, in *Lightoller v. JetBlue Airways Corp.*, No. 23-cv-00361-H-KSC, 2023 U.S. Dist. LEXIS 102158, at *9 (S.D. Cal. June 12, 2023), a plaintiff alleged the interception of her flight pricing information through use of session replay technology constituted a cognizable harm to support her standing to pursue a CIPA claim. The court disagreed, finding flight pricing information is not personal and allegations about it are "insufficient to allege a concrete harm that bears a close relationship to the substantive right of privacy (i.e., an individual's right to control information concerning his or her person)" to establish a concrete harm. *Id.* at *9-10.

Other courts across the country have found no standing associated with tracking clicks, keystrokes, and webpage scrolls using session replay technology, because no sensitive personal identification is accessed. *See, e.g., Straubmuller v. JetBlue Airways Corp.*, No. CV DKC 23-384, 2023 U.S. Dist. LEXIS 155704, at *10 (D. Md. Sept. 1, 2023) (finding plaintiff failed to establish concrete harm because "Plaintiff has not alleged facts establishing targeting or misuse of his personal information" from the use of session replay code); *Cook v. GameStop, Inc.*, No. 2:22-cv-1292, 2023 U.S. Dist. LEXIS 150953, at *12 (W.D. Pa. Aug. 28, 2023) (no standing because "[a]t most, the information that GameStop intercepted related to her product preferences. Product preference information is not personal information" to support standing); *Mikulsky v. Noom, Inc.*, No. 3:23-cv-00285-H-MSB, 2023 U.S. Dist. LEXIS 124719, at *12 (S.D. Cal. July 17, 2023) (plaintiff's conclusory allegation that she disclosed "personal information" captured by session replay code does not allow the court to determine whether plaintiff has a protectable privacy interest in that information to establish Article III standing).

I. Developments in Global Privacy Law

2023 reified a continuation of several global privacy trends. The first trend was the continuing adoption of more national privacy laws (162 national privacy laws are on the books). Second was a tendency for international privacy laws to adhere to the principles that underlie the EU General Data Protection Regulation (GDPR). Finally, we saw the continued search and investment by both private and public actors to reduce the cost, friction, and risk associated with global data flows by participating in data transfer frameworks such as the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules (CBPR) and, most recently, the new EU-U.S. Data Privacy Framework (DPF). The good news for companies this year is that even though sporadic localized privacy standards such as data localization or registering data transfers with a regulator are on the books, regulators are easing some of these requirements for most businesses. Here are three important highlights from 2023 reflecting these trends.

EU-U.S./UK-US

After Schrems II precipitated the invalidation of the EU-U.S. Privacy Shield cross-border personal data transfer agreement in 2020, protracted negotiations resulted in the EU-U.S. Data Privacy Framework, which became effective July 11, 2023. Switzerland has a new separate DPF, which can be added

to EU-U.S. DPF when a company self-certifies. Because this latest agreement came after Brexit, the UK negotiated a corollary UK-U.S. Data Bridge (DB) extension agreement to the DPF effective October 12, 2023. This additional self-certification for DB can be added to DPF self-certification by registering with the USDOC. Once an organization publicly declares its commitment to the DPF, the DB, and/or the Swiss-U.S. Data Privacy Principles, those commitments become enforceable under U.S. law. Since inception, approximately 2,600 organizations have self-certified under the program.

The DPF's goal is to address previous transfer framework deficiencies under EU law by introducing stronger data protection obligations; increasing oversight and enhanced commitments to limit access to data by U.S. authorities; using more robust resolution and redress mechanisms for EU citizens with the possibility of an independent dispute resolution; as well as regular review (and, ostensibly modifications) of the agreement to ensure effectiveness in balancing the need for global digital data transfers with the EU's fundamental rights to privacy and data protection. The DPF principles to which organizations must commit and demonstrate adherence include purpose specification and limitation, notice, choice, data integrity and minimization, access, and onward transfer accountabilities. The DPF also mandates affirmative, express consent for processing sensitive personal data unless an exception applies, such as processing that is in the vital interest of the data subject.

The DPF is administered by the DOC and is available to organizations under the jurisdiction of the FTC or the U.S. Department of Transportation. Therefore, banks, savings and loan companies, and common carriers acting as U.S. data importers are not eligible for the DPF and may still need to enter into alternative standard contractual clauses (SCCs).

Many companies entered into SCCs during the interregnum between valid EU/U.S. cross-border transfer agreements. The DPF covers a broad scope of personal data transfers and is a self-certification program, making it attractive to many businesses over the more tightly scoped and complex SCCs. DPF obligations will evolve over time, while SCCs are static. Still, the DPF and SCCs are not incompatible. Companies considering DPF self-certification that also have standing SCCs may choose to avail themselves of the benefits of the DPF while maintaining the more static SCCs without any jeopardy.

In fact, maintaining both mechanisms may make sense, as the DPF is not without vocal active critics. Ministers and civil society advocates point to a lack of guarantees for private and family life data, the effectiveness of remedies, and the protection of EU data subjects from security breaches. Campaigns, including one by the Schrems-backed organization NYOB, have already begun the fight to invalidate the DPF. Having successfully invalidated to previous frameworks, for companies with significant EU personal data transfers, maintaining current SCCs promotes continuity of operations if the DPF were nullified as a transfer mechanism.

India

India passed the long-awaited Digital Personal Data Protection Act 2023 on August 11, 2023, providing a framework for how companies will need to manage digital data they process in India or when offering goods or services to Indian residents. The final bill pulled back on some of the more onerous burdens for industry and potential friction points for global trade given deep concerns about the effects of the law on the large manufacturing, technology, and outsourced services industries in India. In the end, the final bill did not place restrictions on data transfers and removed data localization requirements for most organizations operating in "trusted" geographies. There are notice and choice requirements for data collection, but the law does not require consent for a broad set of "legitimate uses," including when an individual voluntarily provides personal data for specified goods and services.

The DPDPA applies only to Indian resident, employee, and business-to-business digital or digitized data *"about an individual who is identifiable by or in relation to such data."* The DPDPA also introduces novel privacy language. "Data principals" are data subjects who can make

privacy complaints directly to the DPBI supervisory authority or Indian courts without first seeking redress from the company/data controller or "data fiduciary." The DPBI may designate a data fiduciary as "significant" based on an assessment of relevant factors, including the volume and sensitivity of personal data processed, public order, and the risk to the rights of data principals. All signs indicate that this will be a limited designation. Companies with the significant data fiduciary designation are required to have an in-country data protection officer.

For data breaches, the law does not include a specific impact assessment or "high risk" trigger for breach notification to individuals in the event of a data breach. Instead, it requires notice to both affected individuals and the DPBI without a timeline for reporting. It is expected that a time frame will be included in the regulations. Breach fines range from $6 million to $30 million and will be assessed based on a number of factors, including the degree of harm, failure to maintain adequate privacy/security controls, or inclusion of children's data.

Much of the DPDPA aligns with the data subject rights, principles, and articles of the GDPR. Though the DPDPA consent model is less stringent, like the GDPR and the CCPA, the DPDPA allows "consent managers" registered with the data protection board to act on behalf of data principals as designated by the DPBI. This feature adds additional complexity to the process of verifying data principals and their third-party agents for a potentially huge pool of data principals. While the DPDPA effective date will not be set until the DPBI is established, companies should take stock of when they are processing data as a data fiduciary or controller, explore applicable exceptions, assess risks, and chart their compliance path.

Thailand

Thailand's Personal Data Protection Act (PDPA) went into effect on June 1, 2022. It is enforced by the Personal Data Protection Committee (PDPC). The PDPC made a wise and welcome decision to focus on awareness for the first year of the law's effective date. Enforcement in earnest started in 2023. The law applies to organizations in Thailand that collect, use, disclose, or transfer the data of Thai citizens for commercial purposes. The law applies to organizations outside Thailand that collect, process, or disclose data of Thai citizens for the purposes of offering goods and services or monitoring behaviors in Thailand.

The PDPA largely mirrors the GDPR, including the definitions of personal and sensitive data, lawful purposes for processing, as well as the rights of data subjects. With some exceptions, consent is required before or at the time of data collection,

use, or disclosure. The notice associated with consent must include clear purpose specification, types of data to be collected, retention periods, and categories of persons or entities to whom data may be disclosed. Also, the law requires recipient countries to have adequate data protection standards in place or to obtain consent from the data subject before any data transfer out of Thailand. Data subjects may revoke consent at any time, with some exceptions. Again, organizations doing business globally should ensure they have a flexible, scalable, and extensible data subjects' rights management program in place.

The PDPA requires a breach risk analysis for a privacy/security event involving covered data. Assessments indicating a "high risk" to the "rights and freedoms" of data subjects — for example, potential identity fraud — require that both the PDPA and the data subject be notified, with the former being notified within 72 hours of awareness and the latter without undue delay. A unique requirement in the PDPA and guidance that companies should note is that communication to the PDPC is required when data subject breach notifications are not provided after a data breach. The maximum fine for not reporting a breach to the PDPC is approximately $30,000. Failure to comply with the PDPA may result in civil liabilities, criminal penalties, or administrative fines.

Conclusions

These 2023 capstone laws confirm that global privacy is evolving rather than speciating net new requirements. Authorities may have different recipes. But the same ingredients are used. It is vital that organizations ensure organizational capacity to assess and balance risks and budgets and to stand ready to demonstrate compliance within compressed time frames. Getting there still starts with the basics: actively understanding what data is held; knowing where that data lives; and applying the correct, relevant rules to data management and breach reporting.

If you need specific advice or assistance on how global privacy laws affect your business or on building globally effective programs and procedures, Troutman Pepper's Privacy + Cyber and Regulatory Investigations, Strategy + Enforcement practices are on hand to provide industry-specific and pragmatic advice.