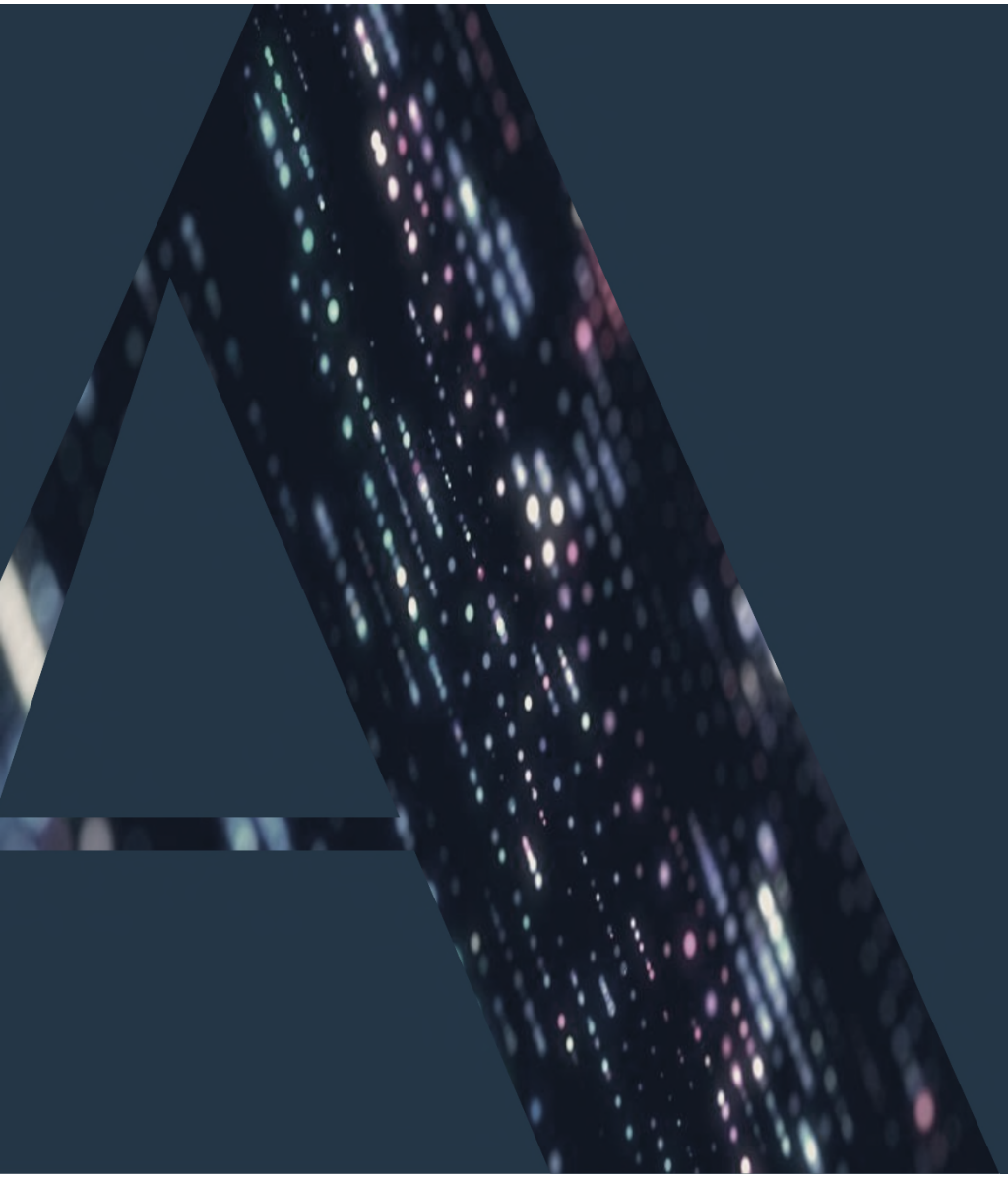


Association of Corporate Counsel, National Capital Region

The Latest Updates in Privacy

March 19, 2024

Natasha Kohne
Partner
Akin

Michelle Reed
Partner
Akin

Moderated by:
Tony Pierce
Partner
Akin

Sheila Pham
Director, Legal - Privacy
RingCentral

Amy Yeung
Vice President
Sallie Mae

Note: panelists are each speaking in their individual capacity and not on behalf of their organizations.

Akin℠

Agenda

- Updates in AI & Emerging Technology
- State Privacy Updates
- California Consumer Privacy Act and California Privacy Rights Act
- Federal Agency Activity
- CCPA Litigation Trends & Strategies
- International Data Protection
- Takeaways

Updates in Emerging AI & Emerging Technology

The White House AI Executive Order

- On October 30, 2023, President Biden issued a comprehensive executive order on AI, laying out guiding principles for federal agencies to apply when developing and deploying AI systems.
- Includes requirements that some AI developers share safety testing results with the government.
- The order reflects the privacy and security priorities present in the earlier Blueprint for an AI Bill of Rights the White House released in October 2022.

"Biden is rolling out the strongest set of actions any government in the world has ever taken on AI safety, security and trust. It's the next step in an aggressive strategy to do everything on all fronts to harness the benefits of AI and mitigate the risks."

- White House deputy chief of staff Bruce Reed

- New Standards for AI Safety and Security
- Privacy protections
- Guidance on equity and civil rights
- Consumer protection
- Employee protection
- Promoting innovation and competition
- International engagement
- Responsible agency use of AI

Federal Agencies on AI

- February 13, 2024 – FTC stated that changing privacy policies to start sharing consumers' data with third parties or using that data for AI training might be considered unfair or deceptive.
- The FTC published a series of blog posts on AI in 2023, issuing a range of warning to companies:
  - Do not blame third party developers for reasonably foreseeable risks
  - Do not exaggerate AI capabilities
  - Use deterrents that go beyond bug corrections or optional features that third parties can undermine
- October 23, 2023 – the FCC announced an inquiry into the impact of AI on robocalls and sought public input into the technology's role in unwanted phone calls and messages.

- Rite Aid Enforcement – on December 19, 2023, the FTC issued an order against Rite Aid for allegedly failing to implement reasonable procedures to prevent consumer harm from its use of facial recognition technology in stores.
  - Delete images and algorithms developed using those images
  - Notify consumers of when their biometric info is collected
  - Data retention – delete biometric info after 5 years
  - Implement data security program
  - Obtain independent third-party assessments
  - Banned from using facial recognition tech for 5 years
- April 25, 2023 – the FTC, Department of Justice (DOJ), Equal Employment Opportunity Commission (EEOC) and the Consumer Financial Protection Bureau (CFPB) published a joint statement emphasizing that their existing enforcement authorities apply to the use of automated systems such as AI. They stated that automated systems may contribute to unlawful discrimination and other violations of federal law.

The State of AI Law (AI law guidance)

EU AI Act

- Tackles risks for specific uses of AI.
- Extraterritorial, sector agnostic.
- Steep noncompliance penalties.

Employment

- New York City.
- Maryland.
- Illinois.
- Department of Justice (DOJ) and Equal Employment Opportunity Commission (EEOC) – both released guidance for use of AI in employment decisions.

Insurance

- Colorado law against algorithmic discrimination in insurance.
- California guidance.

State Privacy Laws

- Provisions governing automated decision-making, which includes tech that facilitates AI-powered decisions.
- State laws such as: California, Connecticut, Colorado, Texas and Virginia.

Federal Guidance

- EO on AI Safety and Security.
- White House AI Bill of Rights.
- National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework.
- Agency statements

EU Draft Regulation on Artificial Intelligence ("EU AI Act")

The AI Act aims to address the risks generated by specific uses of AI through a set of harmonized rules, and in addition imposes obligations and restrictions on general purpose AI systems / foundation models regardless of their use.

The Act has extraterritorial effect, is sector-agnostic, carries steep noncompliance penalties from 7% to 3% of global annual turnover (the upper ceiling is higher than in the GDPR) and applies to multiple stakeholders across the AI value chain, including deployers and providers.

A final vote took place in a plenary session in the EU parliament on March 13, 2024, and the act is expected to be adopted in late spring 2024.

There will be a staggered entry into force, with the provisions relating to prohibited AI systems applying 6 months after adoption, those relating to general purpose AI / foundation models 12 months after adoption, and most of the remaining provisions, including as to high-risk AI systems, 24 months after adoption of the AI Act.

U.S. Executive Order on Sensitive Personal Data

What?	• On 28 February 2024, President Biden issued an Executive Order (**EO**) preventing access to Americans' bulk sensitive personal data and U.S. Government-related data by countries of concern (**CoC**)
Who?	• Directs (i) the Department of Justice (**DOJ**) to prohibit, or otherwise restrict, certain transactions enabling the transfer of sensitive personal data of U.S. citizens to CoC; and (ii) directs federal agencies to take steps to enhance authorities to address data security risks
When?	• No immediately effective provisions; the process for finalizing the regulations implementing the EO is likely to take until at least late in 2024; expect DOJ will publish an Advance Notice of Proposed Rulemaking describing the initial categories of transactions
Why?	• To address a perceived gap in existing national security authorities; increasing concerns about accessing Americans' sensitive personal data and sharing such information with foreign governments
Penalties?	• DOJ will have authority to assess penalties up to the maximum allowable under the International Emergency Economic Powers Act (currently $368,136 per violation)

Covered Countries

- China (including Hong Kong and Macau)
- Russia
- Iran
- North Korea
- Cuba
- Venezuela

Covered Persons

(i) Owned, controlled, subject to jurisdiction / direction of CoC

(ii) Employee or contractor of (i)

(iii) Employee or contractor of CoC

(iv) Primarily resident in territorial jurisdiction of CoC

(v) Designated by DoJ

Prohibited Data Transactions

- Data Brokerage Transactions
- Genomic-Data Transactions

Restricted Data Transactions

- Vendor Agreements Involving Goods / Services
- Employment Agreements
- Investment Agreements

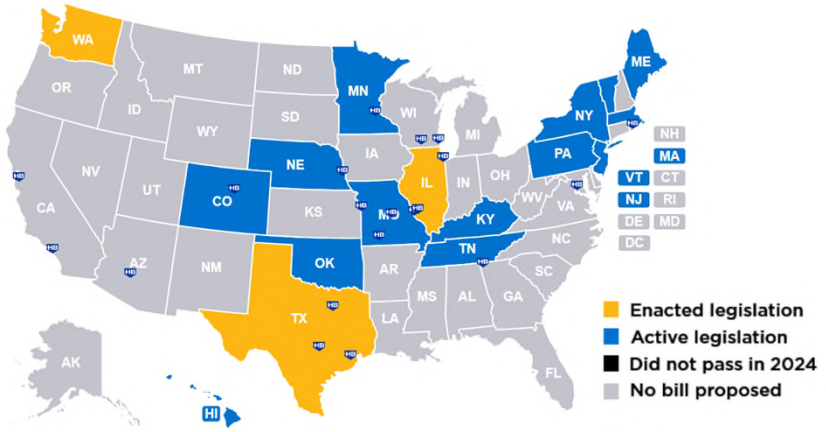
Recent Biometric Privacy Developments

- 2023 was a big year for biometric privacy, with significant developments from class action lawsuits stemming from Illinois' Biometric Information Privacy Act (BIPA).
  - *Cothron v. White Castle System* – Illinois Supreme Court ruled BIPA claims accrue each time data is unlawfully collected and disclosed rather than just the first time (February 17, 2023).
  - *Richard Rogers v. BNSF Railway Company* – an Illinois federal judge vacated an initial $228M fine after determining jurors should have the chance to determine the penalty. The company agreed to settle claims ($75M). (September 15, 2023).
- BIPA filings increased 65% two months after *White Castle*.

BIPA claim statute of limitations is 5 years.

BIPA claims accrue each time data is unlawfully collected and disclosed rather than just the first time.

2024 State Biometric Privacy Law



Last Updated: February 13, 2024

- On May 19, 2023, two plaintiffs filed a class action against a large live-entertainment company for its alleged use of facial recognition software to keep banned individuals out of its venues.
- $650 million for Meta's BIPA settlement—the largest settlement currently on the books—with the U.S. Court of Appeals for the 9th Circuit granting final approval in March 2023.

Rise of Genetic Data Privacy

- States laws increasingly governing specific categories of information like genetic data.

Illinois Genetic Information Privacy Act (GIPA) – increase in GIPA class actions in 2023, alleging required disclosures of employee genetic information.

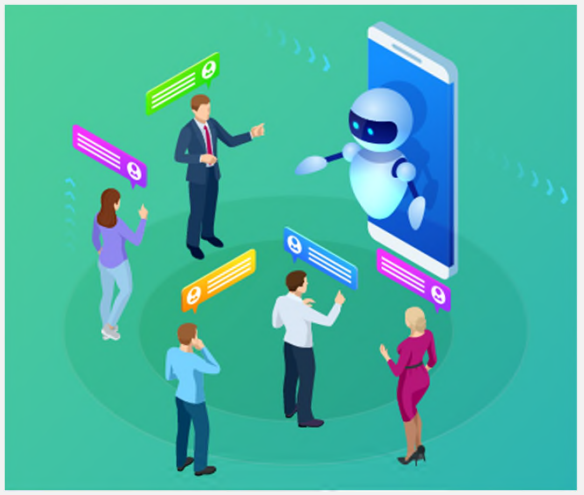
Washington's My Health My Data Act – covered "consumer health data" includes genetic data.

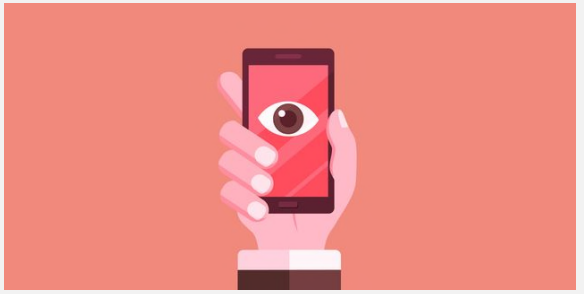
Montana Genetic Information Privacy Act – applies to entities offering consumer genetic testing products and services, or collecting, using or analyzing genetic data.

- FTC on Genetic Data – settlement with 1Health.io over alleged failures to protect genetic data and retroactive changes to privacy policy.
- FTC policy statement describes biometric data "data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body" as including genetic data. Certain use of biometric data could constitute Section 5 violation.

Wiretapping Laws & New Tech

- Similar to 2022, 2023 saw a flood of class action litigation applying state and federal wiretapping laws to modern technologies, such as chatbots, pixels and session replay tools.
  - Session replay tools – Capture a user's entire visit to a webpage, enabling you to recreate or monitor the user's interactions with that page. Often via a third party who provides the tool
- Class action plaintiffs allege that these tools violate wiretapping laws because the consumers have not consented for their interactions with business' website and apps to be intercepted and recorded.
- *Javier v. Assurance IQ, LLC* – U.S. Court of Appeals for the 9th Circuit held that use of session replay tools without prior consent can be a violation of California's wiretapping law, the California Invasion of Privacy Act (CIPA).
- *Jackson v. Fandom Inc.* – Northern District of California judge denied the defendant's motion to dismiss a proposed class action alleging that the defendant, a hosting service for user-generated wikis, violated the federal Video Privacy Protection Act (VPPA) by sharing users' personally identifiable information through pixels.

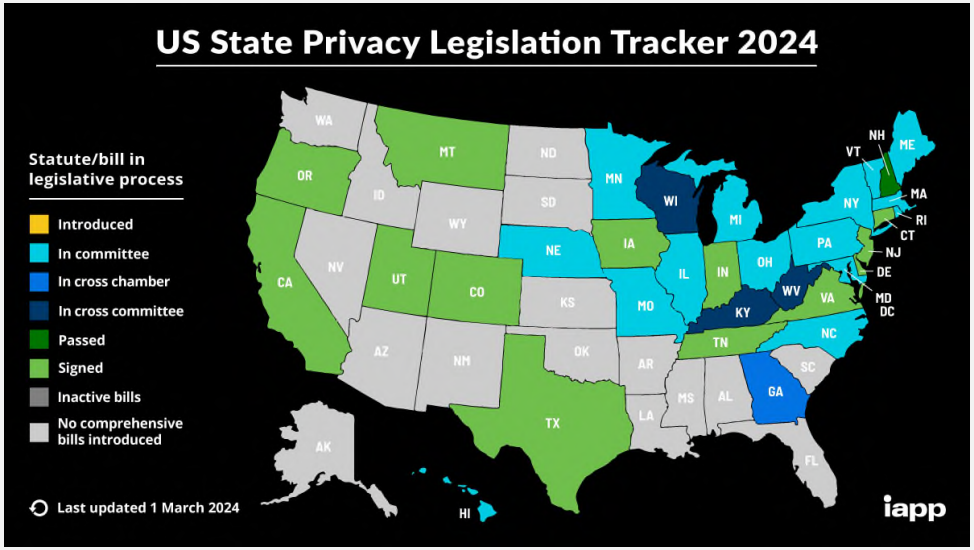




State Privacy Updates

Evolving State Regulations

- In 2023 **7** states enacted comprehensive consumer privacy laws: Delaware, Indiana, Iowa, Montana, Oregon, Tennessee and Texas.
- In 2024 **3** states have comprehensive consumer privacy laws taking effect: Texas, Oregon and Montana.
- All **50** states and U.S. territories have implemented data breach notification laws.
- **40** states introduced or considered **350** consumer-privacy-related bills in 2023, up from 200 in 2022 and 160 in 2021.
- At least **17** states had active comprehensive consumer privacy bills going into 2024.



State Comprehensive Privacy Laws

Law	Enacted Date	Effective Date	Regulations?
California Privacy Rights Act (CPRA)	November 3, 2020	January 1, 2023	Yes
Virginia Consumer Data Protection Act (VCDPA)	March 2, 2021	January 1, 2023	No
Colorado Privacy Act (CPA)	July 7, 2021	July 1, 2023	Yes
Connecticut Data Privacy Act (CTDPA)	May 10, 2022	July 1, 2023	No
Utah Consumer Privacy Act (UCPA)	March 24, 2022	December 31, 2023	No
Texas Data Privacy and Security Act (TDPSA)	June 18, 2023	July 1, 2024	No
Oregon Consumer Privacy Act (OCPA)	July 18, 2023	July 1, 2024	No
Montana Consumer Data Privacy Act (MTCDPA)	May 19, 2023	October 1, 2024	No
Iowa Consumer Data Protection Act (ICDPA)	March 29, 2023	January 1, 2025	No
Delaware Personal Data Privacy Act (DPDPA)	September 11, 2023	January 1, 2025	No
New Jersey Privacy Act (NJPA)	January 16, 2024	January 15, 2025	Yes
Tennessee Information Protection Act (TIPA)	Mary 11, 2023	July 1, 2025	No
Indiana Consumer Data Protection Act (INCDPA)	Mary 1, 2023	January 1, 2026	No

Patterns & Quirks in State Privacy Law

Different Ways States Define "Consumer"

- Most states privacy laws define a "consumer" as an individual who is a resident of the state acting only in an "individual or household context."
- California goes further in the CPRA by adding individuals acting in a "commercial or employment context."

Differences in Exemptions

- All current state laws exempt government agencies.
- Colorado, New Jersey and Oregon do not exempt nonprofits.
- Exemptions are provided by type of entity and type of data and vary by state.

"Sale" of Personal Data

- Some states like Virginia, Utah, Tennessee and Indiana define "sale" as the exchange of personal data "for monetary consideration by a controller to a third party."
- Others like California, Colorado, Connecticut and Texas define "sale" more broadly as including "monetary or other valuable considerations."

Private Right of Action

- So far only California's law contains a private right of action.

Data Protection Assessments

- The majority of states require businesses to conduct a data protection assessment, with the scope and detail required varying by state.

Opt-in/Opt-out Rights for "Sensitive" Data

- The states have different rights pertaining to the processing of sensitive data. Most states (like Colorado, Connecticut, Delaware, Indiana, Montana, Oregon, Tennessee, Texas, and Virginia) feature a right to opt in.

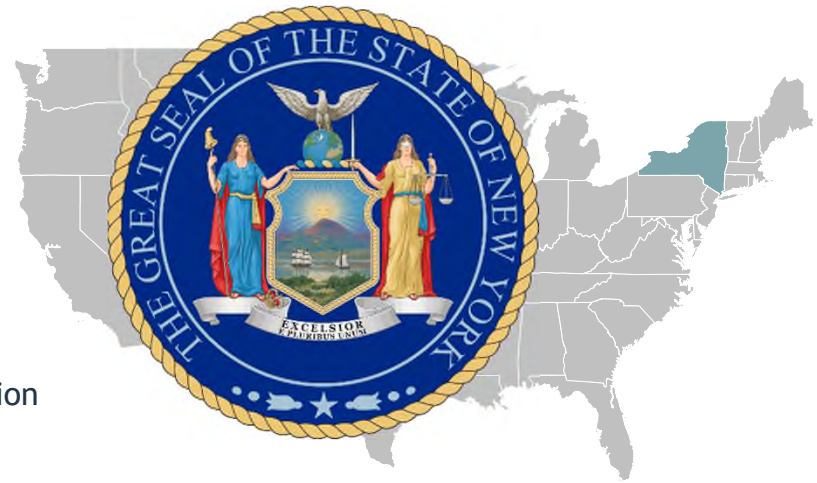
Child Online Safety in the Spotlight

- General trends in litigation and enforcement in Children's Privacy
  - Old protections viewed as insufficient protection in light of new technology.
  - Expanded definitions, increase in more prescriptive, stringent requirements in laws dealing with children online.
  - Children's data key seen as key sensitive data category that regulators are likely to focus on.
- What you need to consider with respect to Children's Privacy
  - Default high privacy settings for children
  - Parental consent requirements, ensure not disclosing data without obtaining separate consent
  - Data minimization, data retention

- **FTC Proposed Children's Online Privacy Protection Act (COPPA) Amendments** - additional requirements attempt to shift burden for children's privacy on to service providers. New restrictions on using/disclosing children's personal information.
- **California AADCA Copycats** – Some states (e.g. Connecticut & Florida) seeking to imitate California's Age-Appropriate Design Code Act (AADCA) (enjoined in September 2023) – requiring online platforms to proactively assess the privacy and protection of children under 18 in the design of any digital product or service that they offer.
- **Age Verification** – At least 7 states passed laws requiring websites with adult content to verify that users are at least 18. Likely to face challenges from First Amendment issues. Texas and Utah passed acts regulating social media companies regarding child users. Requirements typically include age verifications and parental consent to open an account for a user under 18.
- At least 14 states passed laws dealing with child safety online

New York Cybersecurity Measures

- On November 13, 2023, the New York State Department of Health proposed cybersecurity regulations for hospitals to complement HIPAA.
- Earlier on November 1, 2023, the New York Department of Financial Services (NYDFS) finalized amendments to its Part 500 Cybersecurity Regulation ("Amended Cybersecurity Rules")
- The Amended Cybersecurity Rules take effect on a staggered timeline from December 2023 to November 2025. Requirements include:
  1. More obligations for the largest companies
  2. Expanded notification requirements
  3. Additional cybersecurity governance provisions
  4. New requirements for incident response
  5. Obligations for business continuity plans
  6. Expanded risk assessment requirements
  7. Additional access controls and technical controls including data retention
  8. New enforcement provisions



Data Retention: only keep what you need

- Strong data retention is becoming an increasingly core part of privacy risk reduction.
- In February 2023, the FTC's Deputy Chief Technology Officer Alex Gaynor highlighted three best practices for effectively protecting user data privacy and security from recent FTC orders: (i) multi-factor authentication; (ii) requiring encryption and authentication of systems; and (iii) requiring data retention schedules.
- The FTC proposed COPPA amendments include limitations on data retention.
- California:

The CCPA requires businesses to disclose how long they keep each category of personal information or, at a minimum, to disclose the criteria they use to determine retention periods. Companies must limit their data retention to only as long as is ***reasonably necessary*** to fulfill their disclosed purpose for collecting the data. In effect, businesses must implement a maximum retention period for consumers' personal data.

California does not permit businesses to collect additional categories of personal information, or use collected personal information for additional purposes incompatible with the disclosed purpose for which it was collected without providing consumers with required notice.

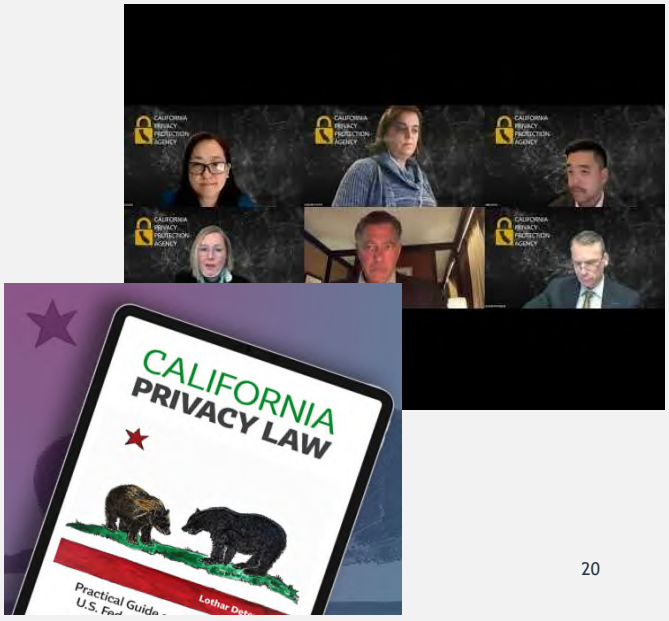
Over-retained data poses a substantial risk under the CCPA.

California Consumer Privacy Act and California Privacy Rights Act

The CPPA's Now Active CPRA Regulations

- On March 29, 2023, the California Privacy Protection Agency (CPPA) Board finalized text of the CPRA Regulations.
- The California Chamber of Commerce filed suit to delay the enforcement until March 29, 2024, on the grounds that voters had intended for enforcement of the regulations to take place 12 months after their finalization.
- Appellate Court sided with the CPPA, ruling enforcement authority should have gone into effect on July 1, 2023.
- **CPPA can now begin enforcing its regulations**, which contain important clarifications for CPRA compliance, such as:

Treatment of opt-out preference signals	Intent behind dark patterns	Notice at collection
Right to limit use/disclosure of sensitive personal information	Processing consumer requests	Data minimization



The CPPA's Remaining Regulations

- The CPPA Board has issued final regulations on 12 out of 15 subject matter areas so far.
- The 3 remaining areas are:
  1. Cybersecurity Audits
  2. Risk Assessments
  3. Automated Decision-making Technology

- Current Status:
  - **Cybersecurity Audits** – received the Board's approval in a December 2023 meeting to advance to formal rulemaking with authorization to make additional changes, with staff to prepare them and return to the Board prior to the 45-day public comment period.
  - **Risk Assessments & Automated Decision-making Technology** – after deciding in the December 2023 meeting that these draft regulations should be sent back to the New CPRA Rules Subcommittee (Rules Subcommittee) for further revision, the Board voted in March to advance both draft regulations to formal rulemaking, with staff to consult with Board members and make additional edits before they will return to the Board again prior to the 45-day public comment period.

State AG/CCPA Regulatory Enforcement

- July 1, 2021 - Office of the California Attorney General (AG) began sending notices of alleged noncompliance to companies, granting 30 days to cure. **As of January 1, 2023, the CCPA no longer requires notice of a violation or an opportunity to cure before filing an enforcement action.*
- January 28, 2022 - AG announces enforcement sweep of loyalty programs.
- August 24, 2022 –AG Bonta announces proposed settlement with Sephora USA, Inc. to resolve claims that Sephora violated the CCPA after failing to cure the alleged violations after 30 days' notice.
- January 27, 2023 – AG announces investigative sweep of mobile apps compliance with consumer rights requirements (including opt-out requests and processing consumer requests submitted through authorized agents).
- July 14, 2023 - AG announces investigative sweep of employee and job applicant data practices.
- July 31, 2023 – CPPA Enforcement Division announces review of data practices of connected vehicles.
- January 26, 2024 - AG announces an investigative sweep of streaming services' compliance with the CCPA's opt-out requirements for businesses that sell or share consumer personal information.
- February 21, 2024 – AG announces settlement with DoorDash to resolve allegations that it violated CCPA notice and opt-out requirements.

Remedies the CA AG may seek:

1. Under the CCPA – injunctive relief, civil penalties: $2,500 per violation or $7,500 for each intentional violation
2. Under UCL – injunctive relief, restitution, civil penalties: $2,500 per violation

Rob Bonta
Current California Attorney General

Other State AG Actions

State Updates

- Connecticut AG Report on CTDPA Enforcement – on February 1, 2023, The Connecticut AG released a report on enforcement actions under the state's new privacy law, emphasizing the importance of curing deficient privacy policies, along with a focus on sensitive data, data brokers and teen data.
- Colorado AG Enforcement Letters – on July 12, 2023, the Colorado AG sent out letters to businesses that the state's privacy law was in force as of July 1, 2023.
- California Age-Appropriate Design Code Act (AADC) Enjoined – U.S. District Court enjoined California from enforcing the AADC, ruling that the act would likely fail First Amendment scrutiny.
- Texas Age Verification Enjoined – U.S. District Court enjoined Texas' age verification law targeting pornography websites, citing First Amendment issues

State AG Data Breach Enforcements:

1. $49.5 Million from Blackbaud – 50 state AGs alleged failures in data security practices. 2020 breach exposing millions of consumers' personal information.
2. $450,000 from U.S. Radiology Specialists – Alleged failure to protect patient data. Breach resulted in ransomware attack affecting more than 92,000 New Yorkers.
3. $6.3 Million from Morgan Stanley – 6 state AG settlement. Alleged failure to employee security measures when decommissioning old devices resulted in exposure of millions of consumers' personal information.
4. $1.4 Million from Immediata Technologies – 33 state coalition alleged failure to timely notify consumers of a coding issue breach and provide sufficient information. 1.5 million patients' sensitive health information exposed.

Federal Agency Activity

Federal Trade Commission

- The Federal Trade Commission (FTC) continues its aggressive regulatory actions in privacy and security, especially targeting commercial surveillance, children's data, AI, biometric data, geolocation and other sensitive data such as health data.
  - Still reviewing comments on its Advanced Notice of Proposed Rulemaking on whether new rules are needed to address potential harms from commercial surveillance and lax data security practices.
  - Announced proposed amendments to the Children's Online Privacy Protection Act (COPPA) Rule at the end of 2023.
- **FTC requirement lists are longer and more detailed**. The agency updated its Safeguards Rule in 2021 (establishing more specific criteria for protection of customer data by nonbanking financial institutions) and again in 2023 (requiring nonbanking financial institutions to report certain data breaches directly to the FTC).
- The FTC has brought hundreds of privacy/cyber enforcement actions so far.

Privacy/Cyber Enforcements

- 1Health.io (September, 2023)
- Rite Aid (December, 2023)
- Ring (May, 2023)
- Amazon (May, 2023)
- Epic Games, Inc. (March, 2023)
- GoodRx Holdings, Inc. (February, 2023)

Enforcement Implications

- Changes in privacy policy require notice
- Responsibility for impact of AI tools
- Specific cybersecurity measures like MFA, encryption, data retention schedule
- Personal liability for executives
- Dark patterns are not affirmative consent

Federal Data Privacy and Security Updates

2023 was a significant year for federal action by several agencies

- **December 20, 2023 - The FTC announces proposed amendments to the Children's Online Privacy Protection (COPPA) Rule.**
- October 30, 2023 – The White House issues an EO on AI on the privacy of Americans' data and for agencies to assess AI risks.
- October 30, 2023 – The SEC charged SolarWinds with failing to properly disclose cybersecurity incidents and risks
- **October 27, 2023 - The FTC amends the Safeguards Rule to require nonbanking financial institutions to report data breaches.**
- **July 26, 2023 - The SEC adopts new disclosure requirements to enhance and standardize public company disclosures regarding cybersecurity risk management and incident reporting.**
- July 20, 2023 – The FTC issues a joint letter with the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) to warn against HIPAA and FTC Act violations in online health portals.
- May 1, 2023 – The FTC publishes a report warning about potential harm to consumers from generative AI tools.
- March 20, 2023 – The FTC publishes a statement warning companies about issues stemming from deepfakes and synthetic media.
- March 15, 2023 – The SEC proposes enhancing Regulation S-P, requiring registered investment advisers to protect customer information.
- February 1, 2023 – the FTC issues publication on practices to address risk from recent FTC orders in privacy and data security cases.
- February 1, 2023 – The FTC issues first-of-its-kind decision enforcement of the Health Breach Notification Rule against GoodRx.
- **January 6, 2023 - The Federal Communications Commission (FCC) proposes updating its data breach requirements.**

What About a Federal Law?

the American Data Privacy and Protection Act (ADPPA) was the most successful attempt yet at establishing a federal consumer data privacy law, but died when Congress adjourned in January 2023.

The FCC Expands Data Breach Reporting

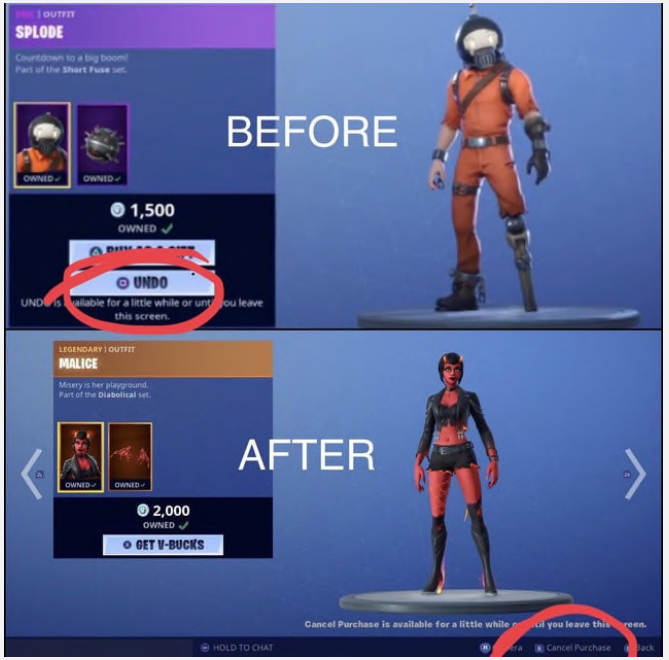
- On December 13, 2023, the FCC issued an order amending its data breach notification rules.
- The updated rules require telecom companies to notify customers about breaches of covered data "without unreasonable delay," eliminating the previous mandatory waiting period.
  - Notify customers – without unreasonable delay after notification to federal agencies, and in no case more than 30 days following reasonable determination of a breach, unless a delay is requested by law enforcement.
- "covered data" includes both customer proprietary network information (CPNI) and Personally identifiable information (PII):
  - It includes information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
- The update broadens the definition of "breach" to include inadvertent access, use or disclosure of covered data.
- Notification to be made to the FCC itself as well as the previously required notification to the Federal Bureau of Investigation (FBI) and Secret Service.

Commerce's "Cyber-Enabled Activities" Rule

- On January 29, 2024, the Department of Commerce (Commerce) issued a proposed rule for U.S. providers of Infrastructure as a Service (IaaS) products and their foreign sellers, implementing EOs on cybersecurity and AI.
- The proposed rule would create new customer identification program requirements for providers of IaaS products outside the U.S. and foreign resellers.
- This customer identification program includes robust "know your customer" requirements, including a requirement that U.S. Providers identify the "beneficial owner" of all accounts (i.e., U.S. and foreign customer accounts) and additional requirements related to foreign-customer accounts.
- The proposed rule also requires U.S. Providers to report information about their non-U.S. customer base to the U.S. government.
- U.S. Providers and their foreign resellers would be required to report to Commerce any "transaction by, for, or on behalf of a foreign person which results or could result in the training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity[.]"

Dark Patterns

- "Dark patterns" – Design practices in online user interfaces that influence users into making choices they would not otherwise have made and that may be against their interests.
- Use of dark patterns to obtain user agreement or to confuse or fatigue a user into staying in an agreement may not be a valid form of consent because the consumer has not been fully or meaningfully informed of their choices. Some examples might include:
  - Ambiguously worded buttons that could trick people into making a different choice than they intended.
  - An unnecessarily lengthy click-through process before customers can cancel a subscription.
  - Requiring scrolling through long documents in order to opt out of data sharing.
  - System defaults to collect more information than a consumer would expect.
- Epic Games – Settled with the FTC for $245 million for alleged use of dark patterns in the Fortnite interface, such as saving credit card information for in-game currency purchases with no purchase confirmation required, setting up hindrances to reversing unauthorized charges. Also required Epic to restructure their billing practices.



SEC Cybersecurity Rule

The SEC has finalized a new cyber governance and disclosure rule it had proposed in 2022:

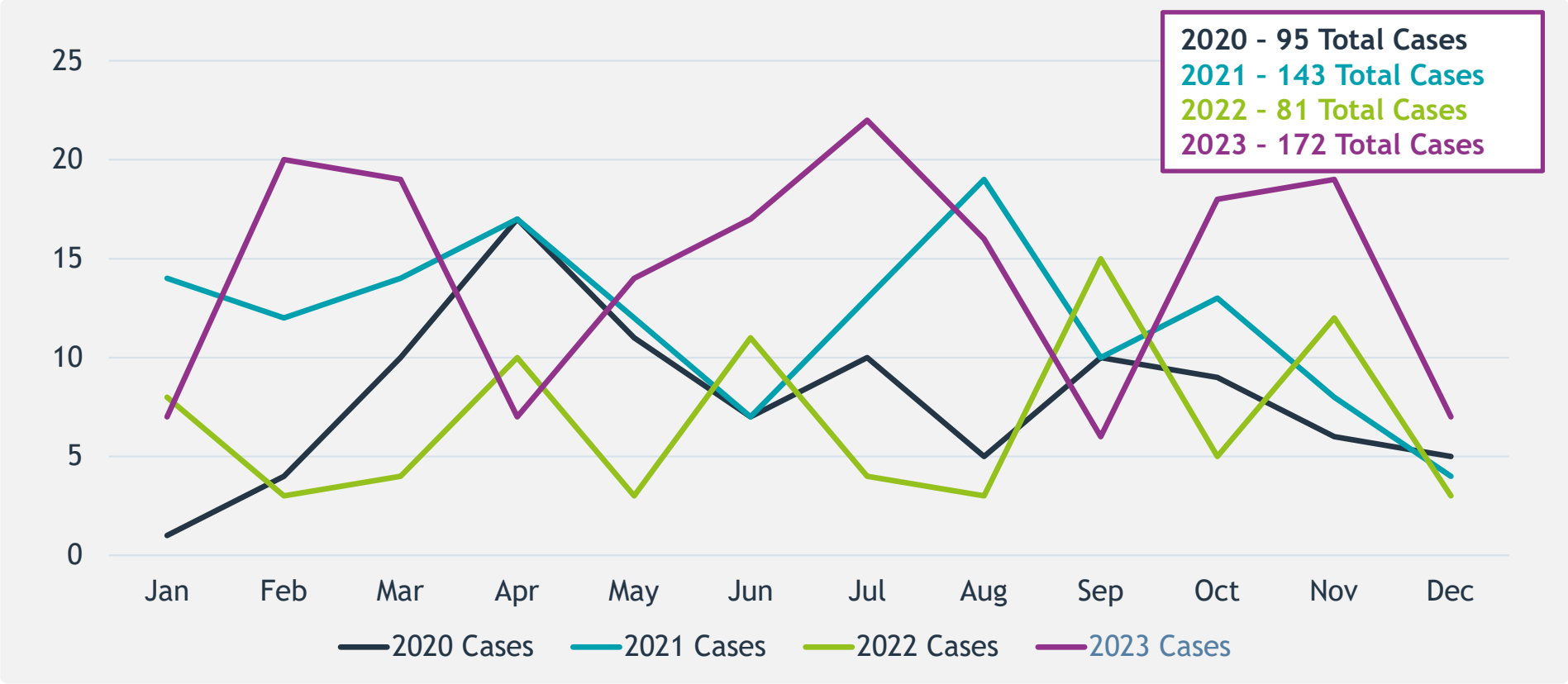
Cybersecurity Incident and Governance Disclosure Obligations for Public Companies – (July 26, 2023)

New rule requires public companies to:

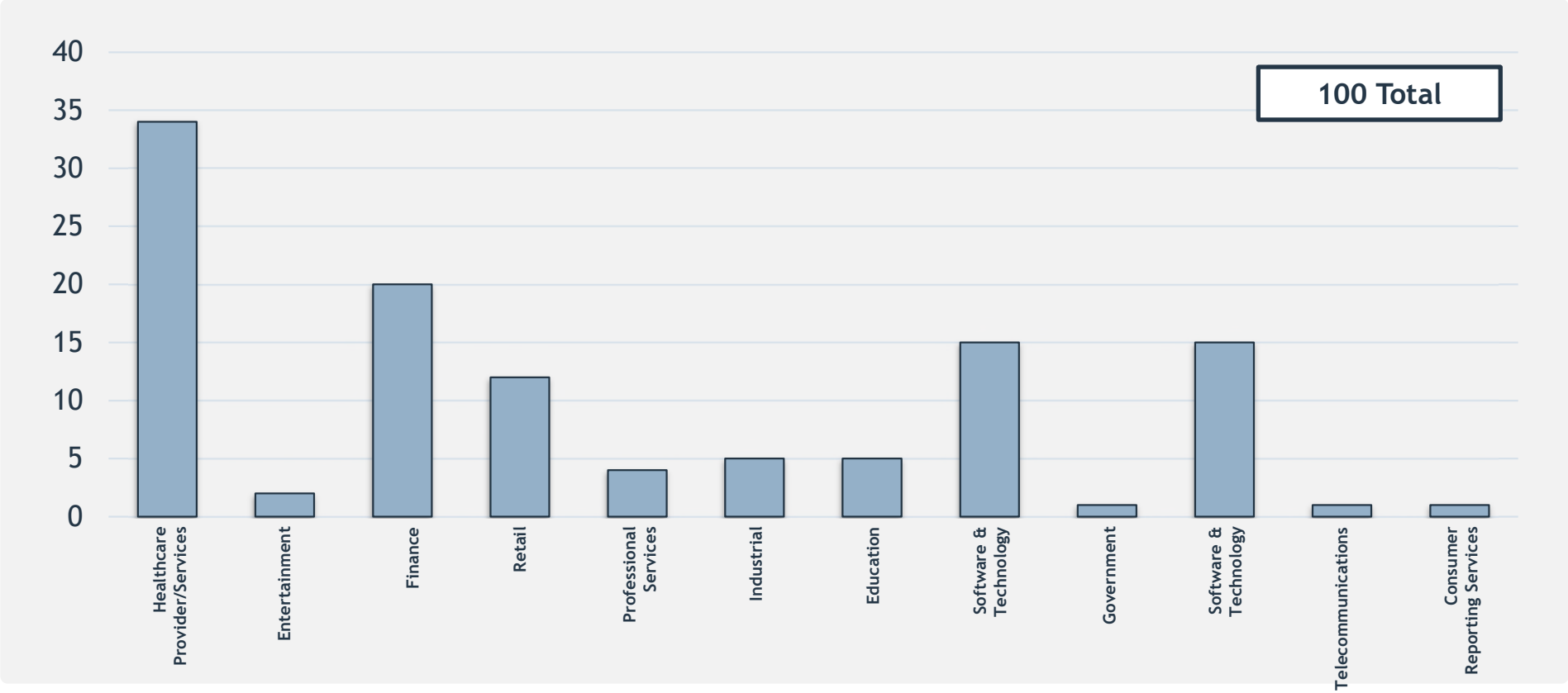
1. Report material cyber incidents within four business days after determining the incident was material
2. Disclose any cybersecurity risks, including from previous cybersecurity incidents, that had a material affect or are reasonably likely to materially affect
3. Describe its cyber risk management policies and procedures
4. Disclose its cybersecurity governance practices
5. Describe board oversight of cybersecurity risks and management expertise
6. Tag the cybersecurity disclosures in Inline eXtensible Business Reporting Language (XBRL)

CCPA Private Right of Action

CCPA Cases Year Over Year: 2020 - 2023



Companies Facing CCPA Claims by Industry in 2023



See Akin's forthcoming CCPA Litigation Report for details and additional statistics.

Where Are CCPA Cases Being Filed?

- Since January 1, 2023, **111** cases have been filed in federal courts, and 61 cases in state court (through December 31, 2023)
- Total companies facing CCPA claims in 2022: **100**
- The majority of cases that cite to the CCPA have been filed in CA courts, but cases have also been filed in numerous other federal courts

Top Courts

Court	Cases
Northern District of California	33
Central District of California	29
State Superior Court, San Diego County	24
State Superior Court, San Francisco County	11

See Akin's forthcoming CCPA Litigation Report for details and additional statistics.

Takeaways

1. Vendor security incidents in healthcare and financial industries may have been the reason for increase in claims.
2. Rise in court using multi-district litigation for big breach cases.
3. TransUnion decision fallout continues to cause issues for Article III standing evaluation.
4. Courts are using differing approaches on what types of data can create a credible risk of imminent harm.
5. Courts are divided on whether the cost of mitigating measures can support standing without an imminent threat of identity theft.
6. Federal courts are likely to find Article III standing where highly sensitive personal data is compromised.
7. California remains the top jurisdiction (both state and federal courts), but cases may be transferred to a defendant's principle place of business.
8. Executive officers face liability for security failures leading to CCPA claims.

International Data Protection

Date 00, 2021

EU-U.S. Data Privacy Framework

- On July 10, 2023, the European Commission (EC) adopted its adequacy decision for the EU-U.S. Data Privacy Framework (DPF) and it entered into force with immediate effect.
- This followed the adoption of the Biden Executive Order on 'Enhancing Safeguards for United States Signals Intelligence Activities' in October 2022, which implemented the DPF and introduced new safeguards, including that personal data can be accessed by US intelligence agencies only when necessary and proportionate.
- The EC's adequacy decision states that there is an adequate level of protection for personal data transferred from the EU to entities participating in the DPF. European entities are therefore able to transfer personal data to participating companies in the US, without having to put in place additional data protection safeguards.
- For individuals in the EU, the DPF also creates new rights, such as the right to obtain access to their data, or obtain correction or deletion of incorrect or unlawfully handled data.
- The DPF is administered by the Department of Commerce and enforced by the Federal Trade Commission.
- Third parties have already indicated that they would challenge the DPF. Not-for-profit organization *nyob*, chaired by Max Schrems (who was behind the invalidation of the EU-U.S. Privacy Shield), announced its intention to challenge the EC's decision by the end of 2023 / early 2024, on the basis that the DPF is a copy of the failed "EU-U.S. Privacy Shield". A challenge by French MEP Philippe Latombe was rejected by the Court of Justice of the European Union in October 2023.

EU Legislative Developments

Digital Markets Act (DMA)

- The DMA's aim is to address certain competition and market issues in the digital space; it started applying for the most part from May 2, 2023.
- On September 6, 2023, the European Commission designated six entities as "gatekeepers" under the DMA: Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft. 22 services provided by those gatekeepers (including Facebook, WhatsApp Messenger and Google) have been designated as "core platform services". No other gatekeepers have been designated yet.
- There are significant obligations on "gatekeepers" under the DMA, including allowing business users to access the data that they generate in their use of the gatekeeper's platform, and providing tools for advertisers and publishers to carry out their own independent verification of their advertisements hosted by the gatekeeper.
- The six designated gatekeepers had to comply with the requirements in the DMA by March 6, 2024.

Data Governance Act (DGA)

- The DGA sets rules for providers of data intermediation services and aims to promote the sharing and re-use of public sector data and to encourage data altruism. The ultimate goal is to increase trust in data sharing.
- In September 2023, the DGA became fully applicable.

Digital Services Act (DSA)

- The DSA's purpose is to rebalance the rights and responsibilities of digital services users, online intermediaries, and online platforms and search engines.
- A wide range of digital services that connect consumers to goods, services or content are caught by the DSA.
- In April 2023, the European Commission designated 17 entities as Very Large Online Platforms (VLOPs) and two as Very Large Online Search Engines (VLOSEs) and a further three platforms were designated as VLOPs in December 2023.
- Since August 2023, the initial 19 VLOPs and VLOSEs have had to comply with the DSA.
- On February 17, 2024, the DSA became applicable to all online intermediaries caught within its scope.

Data Act

- The Data Act (which complements the DGA) is designed to require entities to make data, including non-personal data, accessible to other parties, so that it can be re-used for new purposes.
- Whilst the DGA creates the processes and structures to facilitate data sharing by companies, individuals and the public sector, the Data Act clarifies who can create value from data and under which conditions.
- It entered into force on January 11, 2024, and its provisions will apply as of September 12, 2025.

Other EU Legislative Developments

Digital Operational Resilience Act (DORA)

- DORA sets uniform requirements for the security of network and information systems of companies and organizations operating in the financial sector as well as critical third parties that provide information communication technologies (ICT) related services to them, such as cloud platforms or data analytics services. DORA creates a regulatory framework on digital operational resilience whereby all firms in scope of the Act need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats.
- DORA entered into force on January 16, 2023. It will apply from January 17, 2025.

NIS2 Directive

- The NIS2 Directive seeks to boost the overall level of cybersecurity in the EU and came into force in 2023.
- Member states must adopt and publish the measures necessary to comply with the Directive by October 17, 2024.

Draft E-Privacy Regulation

- The e-Privacy Regulation is intended to update its predecessor, the e-Privacy Directive (deemed the "EU Cookies Law"), as it applies to cookies, digital and online data processing, and telecommunications.
- In July 2021, the European Parliament adopted a derogation from the e-Privacy Directive, aimed at tackling online child abuse material. Other than this, negotiations have not moved forward since May 2021.

Draft AI Liability Directive

- On September 28, 2022, the European Commission proposed a targeted harmonization of national liability rules for AI, making it easier for victims of AI-related damage to get compensation.
- On October 11, 2023, the European Data Protection Supervisor published an Opinion on the proposed Directive with a number of recommendations to ensure individuals receive adequate compensation.
- The draft is going through the motions in the EU legislative process.

Draft Cyber Resilience Act

- On September 14, 2022, the European Commission presented a proposal for a new Cyber Resilience Act to protect consumers and businesses from products with inadequate security features.
- The European Commission, Council and Parliament reached agreement on the text on 30 November 2023 and formal approval is expected in early 2024.
- Upon entry into force, manufacturers, importers and distributors are expected to have 36 months to implement the new requirements (with the exception of 21 months in relation to reporting obligations for incidents and vulnerabilities.)

United Kingdom Developments

- **Online Safety Act 2023**
  - The Act came into force on October 26, 2023. OFCOM is the regulatory authority.
  - It introduces new rules for firms that host user-generated content, i.e., those that allow users to post their own content online or interact with each other, and for search engines, which will have tailored duties focused on minimizing the presentation of harmful search results to users.
  - Penalties include fines of up to £18 million or 10% of the company's annual global turnover, criminal action (and hence imprisonment between 2 to 5 years) against companies and/or senior managers, and business disruption measures. If a company fails to comply with the requirements under an information notice or provides false information in response, senior managers can be held liable if they are found to have failed to take all reasonable steps to prevent it.
- **Revisions to the Network and Information Systems (NIS) Regulations**
  - On November 30, 2022, the UK government confirmed that the NIS Regulations will be strengthened to protect essential and digital services against increasingly sophisticated and frequent cyberattacks – mirroring the response by the EU with the development of the EU NIS2 Directive (as the UK does not need to adopt the EU law following Brexit).
  - Under the current regime, organizations that fail to put in place effective cybersecurity measures can be fined as much as £17 million for material noncompliance.
- **Regulation of general-purpose AI systems**
  - The U.K government announced that it may introduce "future targeted, binding requirements for most advanced general-purpose AI systems", and asked key regulators in February 2024 to state "how they are responding to AI risks and opportunities" by the end of April 2024.

United Kingdom Developments (Cont.)

- **Product Security and Telecommunications Infrastructure Act 2022**
  - The Act makes provision about the security of internet-connectable products and products capable of connecting to such products.
  - The Act received Royal Assent on December 6, 2022 and will enter into force on April 29, 2024.
  - The Act is the first of two pieces of legislation relating to the UK's consumer connectable product security regime.
- **Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023**
  - These Regulations are made under the Act above and outline the security requirements that manufacturers of UK consumer connective products must ensure their products adhere to.
  - The Regulations will apply from April 29, 2024.
- **Data Protection and Digital Information Bill**
  - The Bill is intended to update and simplify the U.K.'s data protection framework by amending the existing U.K. GDPR and Data Protection Act 2018.
  - The Bill is still proceeding through the UK Parliament but is expected to come into force in 2024.
- **Digital Markets, Competition and Consumers Bill**
  - The Bill is aimed at introducing a world-leading regulatory regime in digital markets, focused on preventing anti-competitive activity and boosting innovation. It will give new powers to the Competition and Markets Authority to challenge anti-competitive conduct.
  - The Bill is currently proceeding through the UK Parliament and is expected to come into force in 2024.

GCC High-Level Comparison

	UAE	KSA	Oman	Kuwait	Bahrain	Qatar
Primary Legislation	Federal Decree Law No. 45 of 2021 on the Protection of Personal Data	Personal Data Protection Law Royal Decree M/19 of 9/2/1443H; Cabinet Resolution No. 98 of 7/2/1443H	Sultani Decree No. 6 of 2022 on the Issuance of Personal Data Protection Law	Kuwait Decision No. 42 of 2021 on the Data Privacy Protection Regulation	Bahrain Law No. 30/2018 issuing the Law on Personal Data Protection	Law No. 13 of 2016 on Personal Data Privacy Protection
Executive regulations?	Pending	In force	In force	Not Applicable	Ministerial decisions issued	Ministry of Transport and Communications published new guidelines in 2020
In force?	Yes	Yes	Yes	Yes	Yes	Yes
Regulator	UAE Data Office	Saudi Authority for Data and Artificial Intelligence	Ministry of Transport, Communications and Information Technology	Telecommunication and Information Technology General Authority	Personal Data Protection Authority	Ministry of Transport and Communication
Maximum Penalties	To be prescribed in cabinet decision	SAR 10,000,000 and imprisonment	OMAR 500,000	Penalties prescribed under Kuwait Law No. 34 of 2014 (as amended)	BHD 20,000 and imprisonment	QAR 5,000,000
Cross- border transfer restrictions?	Yes	Yes	Yes	Yes	Yes	Yes
Data breach notification requirements?	Yes	Yes	Yes	Yes	Yes	Yes

Major Legislative Developments Around the World

Significant new data privacy regimes on the rise globally—a number of countries have updates and other actions within regimes already in force, while some have measures still pending.

Already in Force

- **China**
- **United Arab Emirates (UAE)**
- **Brazil**
- **Qatar**
- **Kuwait**
- **South Korea**
- **Bahrain**
- **Oman**
- **Thailand**
- **Indonesia**
- **Botswana**
- **India**
- **Rwanda**
- **Uganda**
- **Ecuador**
- **Russia**
- **Belarus**
- **Japan**

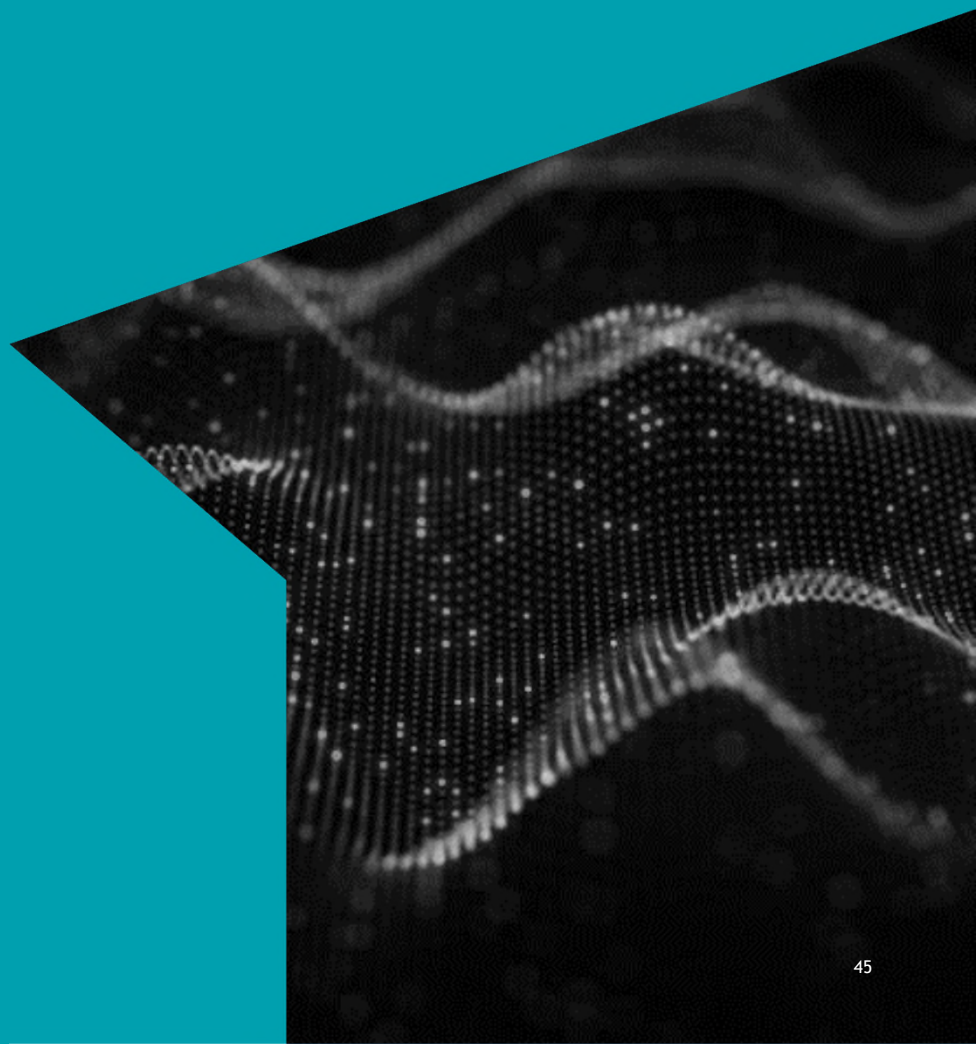
Pending

- **United Arab Emirates**: On November 27, 2021, the UAE announced the issuance of Federal Decree Law No. 45 of 2021 regarding personal data protection, which serves as the UAE's first comprehensive federal data protection law regulating the collection and processing of personal data in the UAE. The law entered into effect on January 2, 2022, but shall only became enforceable six months following the issuance of executive regulations by the UAE Data Office, and no such regulations have as yet been issued.
- **Saudi A**rabia: On September 24, 2021, Saudi Arabia published the Personal Data Protection Law, which serves as the country's first comprehensive national data protection legislation that will regulate the collection and processing of personal data. The law was implemented pursuant to Royal Decree M/19 of 9/2/1443H (i.e., September 16, 2021) and was due to become effective on March 23, 2022, although the full enforcement of the law has since been postponed until March 17, 2023.
- **Jordan**: On December 29, 2021, the Council of Ministers of the Hashemite Kingdom of Jordan approved a draft law on the protection of personal data. In January 2022, the draft law was published on the Legislation and Opinion Bureau's website, although the draft law remains subject to the approval of the parliament and the King.
- **India**: On August 11, 2023, the Government of India enacted the Digital Personal Data Protection Act 2023, but further governmental actions may be required to make that Act effective.
- **Switzerland**: The revised Federal Act on Data Protection and the revised Data Protection Ordinance came into force on September 1, 2023.

China’s PIPL, DSL and Cybersecurity Law

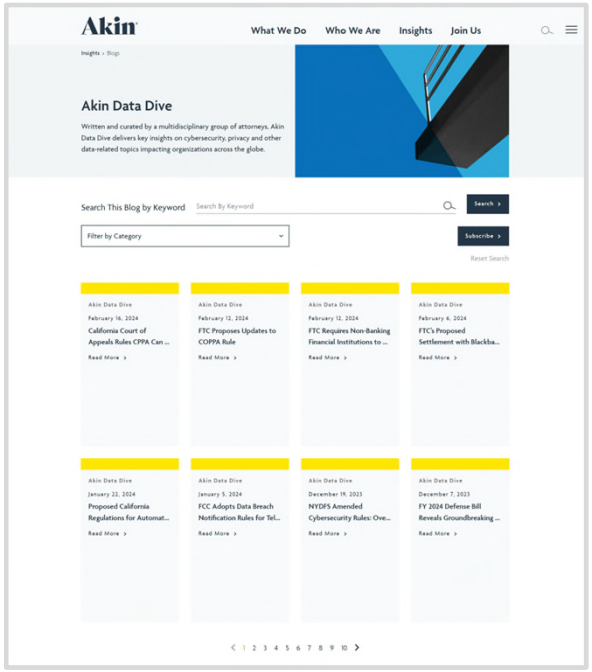
- To better implement China’s data protection laws (the PIPL, Data Security Law (DSL) and Cybersecurity Law, and in particular the cross-border requirements in those laws), the following rules were issued in 2023, among others:
  - For the cross-border data transfer, the Draft Provisions on Regulating and Facilitating Cross-border Data Flow was issued to solicit public comments by October 15, 2023. The draft provides some exceptions where the requirement of security assessment, standard contract for personal information, and personal information protection certification are not required. The final version is soon to be published.
  - For the cross-border data transfer standard contract, the Measures for the Standard Contract for Outbound Cross-Border Transfer of Personal Information was issued on February 22, 2023 and took effect on June 1, 2023. The Guidelines for Filing the Standard Contract for Outbound Cross-Border Transfer of Personal Information (First Edition) was also published to guide and help personal information processors to file the standard contract on May 30, 2023, which took effect on the same day. Local provinces have also successively issued guidelines for record-filing of the standard contract within the region.
  - For the cybersecurity review, the Trial Administrative Measures of Overseas Securities Offering and Listing by Domestic Companies was issued on February 17, 2023 and took effect on March 31, 2023. The trial measures require the provision of personal information and important data to overseas parties in relation to overseas offering and listing of domestic companies shall be in compliance with relevant data protection laws. Different industries have also introduced cybersecurity measures suitable for specific industries, including securities and futures industries, etc.
    - In addition, China announced that Micron’s products failed to pass the cybersecurity review on May 21, 2023, and as a result, the operators of critical information infrastructure in China must stop procuring Micron’s products.

Takeaways



Akin Resources

- Global and U.S. cybersecurity and privacy updates through Akin's AG Data Dive Blog and client alerts.



Team Contact Information

Natasha Kohne, CIPP/U
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle Reed, CIPP/US
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Amy Yeung
Vice President
Sallie Mae

Anthony T. Pierce, Moderator
Partner
apierce@akingump.com
Washington, D.C.
+1 202.887.4411

Sheila Pham
Director, Legal – Privacy
RingCentral

GDPR vs. CCPA vs. CPRA (Appendix)

Components	General Data Protection Regulation (GDPR)	California Consumer Privacy Act (CCPA)	California Privacy Rights Act (CPRA)
Right to Restrict Use of Your Sensitive Personal Information (PI)	✓	✗	✓
Right to Correct Your Data	✓	✗	✓
Storage Limitation: Right to Prevent Companies from Storing Info Longer than Necessary	✓	✗	✓
Data Minimization: Right to Prevent Companies from Collecting More Info than Necessary	✓	✗	✓
Provides Transparency Around “Profiling” and “Automated Decision Making”	✓	✗	✓
Establishes Dedicated Data Protection Agency to Protect Consumers	✓	✗	✓
Restrictions on Onward Transfer to Protect Your Personal Information	✓	✗	✓
Requires High-Risk Data Processors to Perform Regular Cybersecurity Audits	✓	✗	✓
Requires High-Risk Data Processors to Perform Regular Risk Assessments	✓	✗	✓
Appoints Chief Auditor with Power to Audit Businesses’ Data Practices	✓	✗	✓
Protects California Privacy Law from Being Weakened in Legislature	N/A	✗	✓