



The Latest Updates in Privacy

Association of Corporate Counsel, National Capital Region

March 2, 2023

Natasha Kohne
Partner
Akin Gump

Michelle Reed
Partner
Akin Gump

Molly Whitman
Counsel
Akin Gump

Mary Blatch
Senior Privacy Counsel
StockX

Moderated by:
Tony Pierce
Partner
Akin Gump

AGENDA

- State Privacy Updates
- California Consumer Privacy Act and California Privacy Rights Act
- Emerging Technology Updates
- Federal Agency Activity
- CCPA Private Right of Action
- International Data Protection
- Takeaways

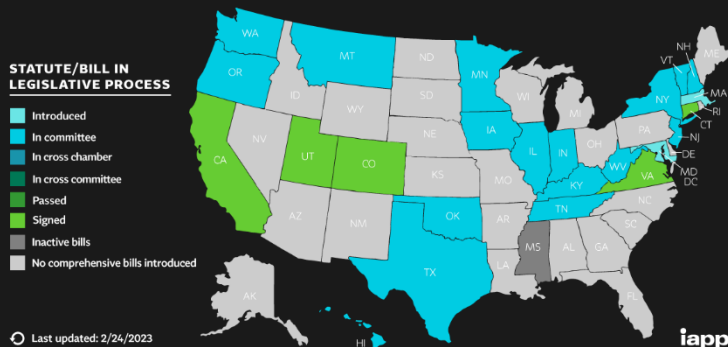


State Privacy Updates

Evolving State Regulations

- Heading into 2023, **5** states have comprehensive privacy legislation taking effect.
- All **50** states and U.S. territories have implemented data breach notification laws.
- **35** states and Washington, D.C. introduced **200** consumer-privacy-related bills in 2022, up from 160 in 2021 and 30 in 2020.
- At least **19** states have active comprehensive consumer privacy bills in 2023, including Massachusetts, Hawaii, Kentucky, Texas and Oklahoma.

US State Privacy Legislation Tracker 2023



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

Patterns & Quirks in State Privacy Law

Different Ways States Define “Consumer”

- Virginia, Colorado, Connecticut and Utah’s 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 five current state laws exempt government agencies.
- Colorado is the only one that does not exempt nonprofits.
- Exemptions are provided by type of entity and type of data and vary by state.

“Sale” of Personal Data

- Virginia and Utah define “sale” as the exchange of personal data “for monetary consideration by a controller to a third party.”
- California, Colorado and Connecticut define “sale” more broadly as including “monetary or other valuable considerations.”

Private Right of Action

- Most laws and proposed bills do not contain a private right of action. California’s law does, as do bills in Massachusetts, New York, Washington and Oregon.

Data Protection Assessments

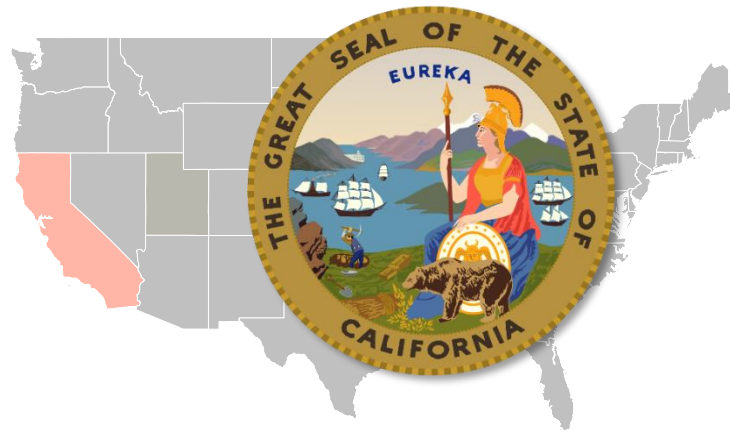
- Of the five current state laws, Utah is the only one that does not require businesses to conduct a data protection assessment. Most of the proposed bills require them, with the scope and detail required varying by state.


Opt-in/Opt-out Rights for “Sensitive” Data

- The states have different rights pertaining to the processing of sensitive data. Virginia, Colorado and Connecticut feature a right to opt in.

California Age-Appropriate Design Code Act

- Enacted August 30, 2022, the California Age-Appropriate Design Code Act (CAADCA) requires online platforms to proactively assess the privacy and protection of children in the design of any digital product or service that they offer.
- Applies to businesses that provide an online service, product or feature likely to be accessed by children under 18, based on similar law in the United Kingdom (the Age-Appropriate Design Code). Broader than the Children's Online Privacy Protection Act (COPPA), with broader definition of "child"—a consumer under the age of 18.
- Five states also currently have legislation to increase protections for children's data, including New York.
- Takes effect July 1, 2024. Requirements include:
 1. Data Protection Impact Assessments
 2. High privacy configuration by default
 3. Estimate ages of child users
 4. Provide clear privacy policy
 5. Prominent tools for exercising rights
 6. Clearly identify tracking signals
 7. No collecting/disclosing geolocation unless strictly necessary.
- Civil Penalties: Up to \$2,500 per affected child for negligent violations and up to \$7,500 per affected child for intentional violations.





California Consumer Privacy Act and California Privacy Rights Act

GDPR vs. CCPA vs. CPRA

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	✗	✓

The CPPA's Proposed CPRA Regulations

- The California Privacy Protection Agency (CPPA) Board has finalized text of the CPRA Regulations and submitted them to the Office of Administrative Law (OAL) for approval. Public comments must be received by March 27, and the OAL has 30 days to approve. The earliest the Regulations could become effective is April 2023.
- The Regulations contain important clarifications for CPRA compliance, such as:
 1. Treatment of opt-out preference signals
 2. Intent behind dark patterns
 3. Notice at collection
 4. Right to limit use/disclosure of sensitive personal information
 5. Processing consumer requests
 6. Data minimization

State AG/CCPA Regulatory Enforcement

- Former California Attorney General (AG) Xavier Becerra made good on his promise to “descend on” non-CCPA compliant businesses. On July 1, 2021, the Office of the AG began sending notices of alleged noncompliance to companies, granting 30 days to cure. The current California AG, Rob Bonta, posted a list of twenty-seven examples of these enforcement actions, providing examples of curative actions.
- On July 19, 2022, a coalition of ten state attorneys general, led by Bonta, wrote Congress to demand that any national consumer privacy law not preempt state legislation, stating that a national law should set “a floor, not a ceiling,” for privacy regulation.
- On August 24, 2022, in the first public enforcement action by the AG under the CCPA, California AG Bonta announced a 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.
- Without admitting or denying fault, Sephora will pay \$1.2 million and commit to comply with the CCPA and relevant provisions of the CPRA when they become operative on January 1, 2023.

Sephora’s alleged violations:

1. Failing to disclose selling of consumer personal information.
2. Claiming to not sell consumers’ information when it did have business relationships with third parties to serve targeted ads based on consumer browsing history.
3. Failing to provide a conspicuous “Do Not Sell My Personal Information” link in either its app or website.

Xavier Becerra
Former California Attorney General



Rob Bonta
Current California Attorney General



Other State AG Actions

- **Google v. 40 State AGs** – On November 14, 2022, Google agreed to a \$391.5 million settlement with the AGs of 40 U.S. states over location tracking controls available in its user account settings, alleging violation of state consumer protection laws.
 - Beginning in 2023, Google will display key information about location tracking in a way that is “unavoidable for users” (i.e., not hidden) and will show contextual information whenever users make a choice about location tracking.
- **Arizona v. Google** – Google agreed to pay \$85 million to settle allegations that it was illegally misleading users about location data tracking, breaching Arizona’s Consumer Fraud Act by continuing to track users who had opted out of location history setting.
- **Texas v. Google** – Amended geolocation suit on May 19, 2022, to include “Incognito Mode” as a Deceptive Trade Practices Act violation.

New York AG Data Breach Enforcements:

1. \$200,000 from Herff Jones – Alleged failure to protect consumer data. Breach of credit card information of thousands of Herff Jones consumers, including more than 40,000 New Yorkers.
2. \$1.9 Million from E-Commerce SHEIN and ROMWE Owner Zoetop – Alleged failure to protect data. Breach in which 39 million SHEIN accounts and 7 million ROMWE accounts were stolen, including more than 800,000 New Yorkers.
3. \$1.25 million from Carnival Cruise Line – Multistate settlement. Alleged poor security practices resulting in a 2019 data breach that exposed the data of 180,000 Carnival employees and customers nationwide, including 6,575 New Yorkers.

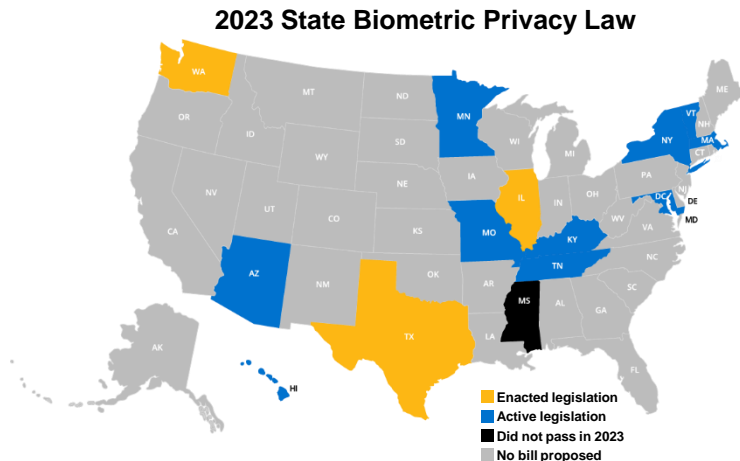
Emerging Technology Updates



Recent Biometric Privacy Developments

- Biometrics protections continue to be added to state data breach notification laws (Texas, New York, California, Washington, Arkansas).
 - New York’s biometrics law (NYC Admin. Code §§ 22-1201–1205), which went into effect July 9, 2021, requires businesses to notify customers of the use of biometric identifiers and prohibits the sale of biometric identifier information.
 - State biometric litigation: Texas AG suit against Meta for alleged violations of state’s biometric privacy law (February 14, 2022).
- Biggest trend continues to be class action lawsuits stemming from Illinois’ Biometric Information Privacy Act (BIPA).
- BNSF case – \$228 million BIPA jury verdict over collecting truck drivers’ fingerprints (October 12, 2022).

Illinois Supreme Court Ruling: Feb. 17, 2023, BIPA claims accrue each time data is unlawfully collected and disclosed rather than just the first time.



- \$92 million for the TikTok BIPA multidistrict litigation, with final settlement approval granted in August.
- \$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 having granted final approval in March.

Wiretapping Laws & New Tech

- A flood of recent class action litigation has sought to apply state wiretapping laws to modern technologies, especially **chatbots** 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 are alleging that session replay tools violate state wiretapping laws because the consumers are unaware of this activity recording and have not consented.
- Similar claims involving chatbots recording and learning user communications without user consent.
- *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).



The State of AI Law

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

EU AI Act



- 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.

Employment



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

Insurance



- Provisions governing automated decision-making, which includes tech that facilitates AI-powered decisions.
- California, Connecticut, Colorado and Virginia.

State Privacy Laws



- White House AI Bill of Rights.
- National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework.

Federal Guidance





Federal Agency Activity

Federal Trade Commission

- The Federal Trade Commission (FTC) is “[c]oncerned that many companies do not sufficiently or consistently invest in securing the data they collect from hackers and data thieves” and “require people to sign up for surveillance as a condition for service” (according to the FTC’s Aug. 2022 *Fact Sheet on Commercial Surveillance and Data Security Rulemaking*).
- In August 2022, the FTC issued an Advanced Notice of Proposed Rulemaking to seek public comment on whether new rules are needed to address potential harms stemming from commercial surveillance and lax data security practices. These comments closed November 21, 2022.
- The agency has adopted a stronger focus on sensitive data, such as children’s data (Epic Games, WW International) & geolocation (Kochava), along with dark patterns (Epic Games).
- FTC requirements are becoming more detailed. The agency updated its 2003 Safeguards Rule, establishing more specific criteria for protection of customer data by nonbanking financial institutions. Further updates concerning the reporting of cybersecurity breaches to the FTC are under consideration.
- The FTC has brought hundreds of cyber/privacy enforcement actions so far, including:
 - GoodRx Holdings, Inc. (February 1, 2023)
 - Chegg (January 26, 2023)
 - Drizly, LLC., In the Matter of (January 10, 2023)
 - Epic Games, Inc. (December 19, 2022)
 - Kochava, Inc. (August 29, 2022)
 - CafePress, In the Matter of (June 24, 2022)
 - Twitter, Inc. (May 25, 2022)



Federal Data Privacy and Security Updates

2022 was a significant year for federal action by several agencies.

- **January 6, 2023 – The Federal Communications Commission (FCC) proposes updating its data breach requirements.**
- December 14, 2022 – The FTC holds a meeting on cybersecurity, which discusses some measures that the agency considers cybersecurity best practices.
- November 15, 2022 – The FTC announces it is delaying compliance deadline for eight of the amendments to the Safeguards Rule until June 9, 2023.
- October 27, 2022 – The Consumer Financial Protection Bureau (CFPB) announces it is writing a regulation to implement Section 1033 of the Dodd-Frank Act, which authorizes the CFPB to prescribe how consumers may access information about themselves from their financial service providers.
- **September 15, 2022 – The FTC (pursuant to a request by Congress) released a report on “dark patterns” obscuring consumer privacy choices.**
- **August 11, 2022 – The FTC issues Advanced Notice of Proposed Rulemaking on commercial surveillance and data security practices, a new privacy rule.**
- August 11, 2022 – The CFPB confirms financial companies may violate federal consumer financial protection law when they fail to safeguard consumer data.
- July 20, 2022 – The America Data Privacy and Protection Act (ADPPA) advances to the House of Representatives. It is not brought to a vote.
- May 19, 2022 – The FTC releases a policy statement on COPPA enforcement and its intention to enforce limits on collection, use and retention of children’s data.
- March 15, 2022 – Biden signs the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA); critical infrastructure providers in areas such as financial services and information technology will have a 72-hour reporting requirement for cyber incidents.
- **March 9, 2022 – The Securities and Exchange Commission (SEC) proposes cybersecurity rules for public companies.**
- **February 9, 2022 – The SEC proposes cybersecurity rules for registered investment advisors and funds.**

The FCC's Proposed Data Breach Reporting

- On January 6, 2023, the FCC released a Notice of Proposed Rulemaking updating its data breach reporting requirements.
- The updated rules would require telecom companies to notify customers and regulators about breaches of customer proprietary network information (CPNI) “without unreasonable delay,” eliminating the current mandatory waiting period.
 - The Communications Act of 1934 defines CPNI very broadly:

It includes information relating to the quantity, technical configuration, type, destination, location and amount of use of a a telecom service as well as certain information contained in customers’ bills.
- The update would broaden the definition of “breach” to include inadvertent access, use or disclosure of CPNI.
- Notification would have to be made to the FCC itself as well as the currently required notification to the Federal Bureau of Investigation (FBI) and Secret Service.

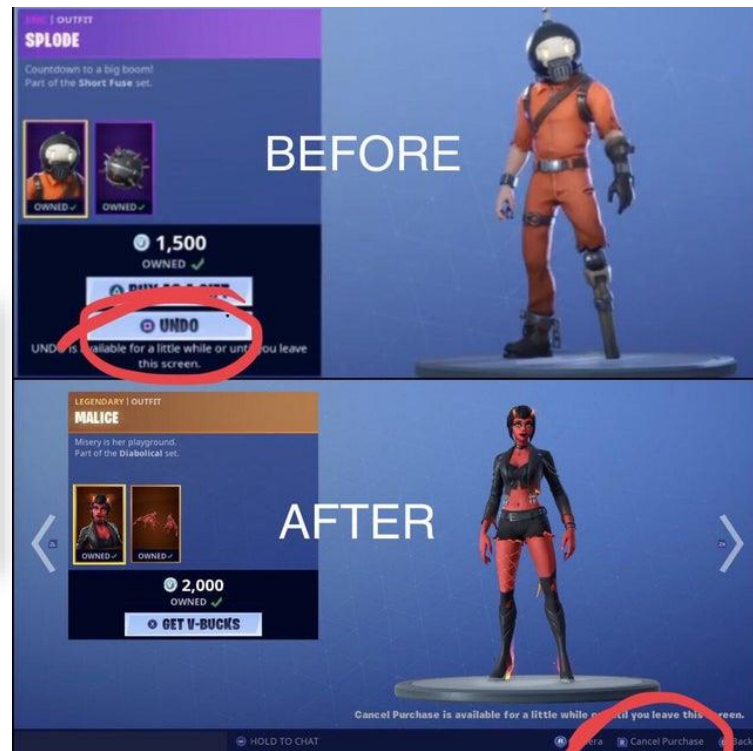


Dark Patterns

- “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.



Attempt at a Federal Law: The ADPPA

- One of the highlights of data privacy in 2022, the American Data Privacy and Protection Act (ADPPA) was the most successful attempt yet at establishing a federal consumer data privacy law.
- The bill died when Congress adjourned in January 2023 but progressed surprisingly far, advancing to the House but never being brought to a vote.
- Features of the ADPPA included:

- A broad scope: Covered entities included any entity or person that alone or jointly determines the purposes and means of collecting, processing or transferring covered data and is subject to the FTC Act, as well as common carriers and nonprofits.
- A duty of loyalty requiring data minimization, and adoption of privacy by design principles. These requirements were more prescriptive than the GDPR, giving specific considerations covered entities should weigh.
- Affirmative express consent from data subjects before collecting, processing, or transferring certain personal data.
- A private right of action going into effect 4 years after the law's enactment.
- Preemption of state laws (except for BIPA and the Illinois Genetic Information Privacy Act).



- Preemption was a contentious issue, and likely responsible for the bill's death.
- Although unsuccessful, the ADPPA will inform future federal efforts, and demonstrates the significant bipartisan support for a federal law.

The SEC's Proposed Cybersecurity Rules

The SEC is looking to finalize new proposed cyber rules (both expected April 2023):

Cybersecurity Incident and Governance Disclosure Obligations for Public Companies – (March 2022)

Proposed rules would require public companies to:

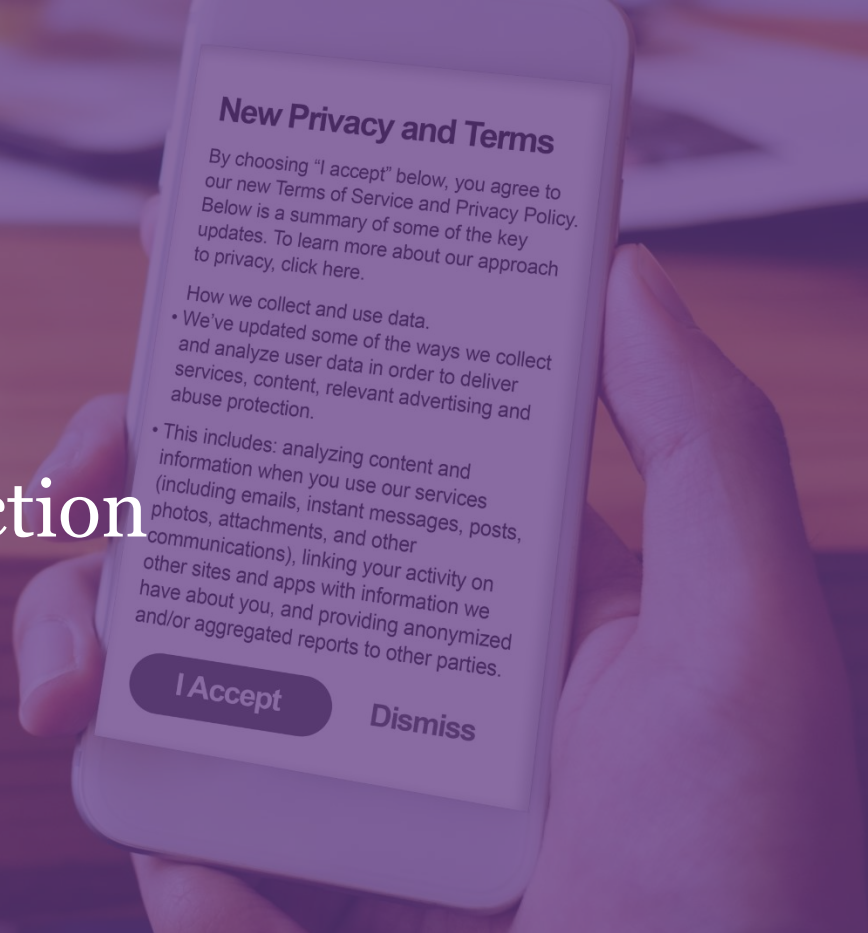
1. Report material cyber incidents within four business days after determining they had experienced an incident.
2. Provide periodic updates of previously reported cyber incidents.
3. Describe its cyber risk management policies and procedures.
4. Disclose its cybersecurity governance practices.
5. Disclose cybersecurity expertise on the board of directors.

Cybersecurity Requirements for Investment Advisers and Companies – (Feb 2022)

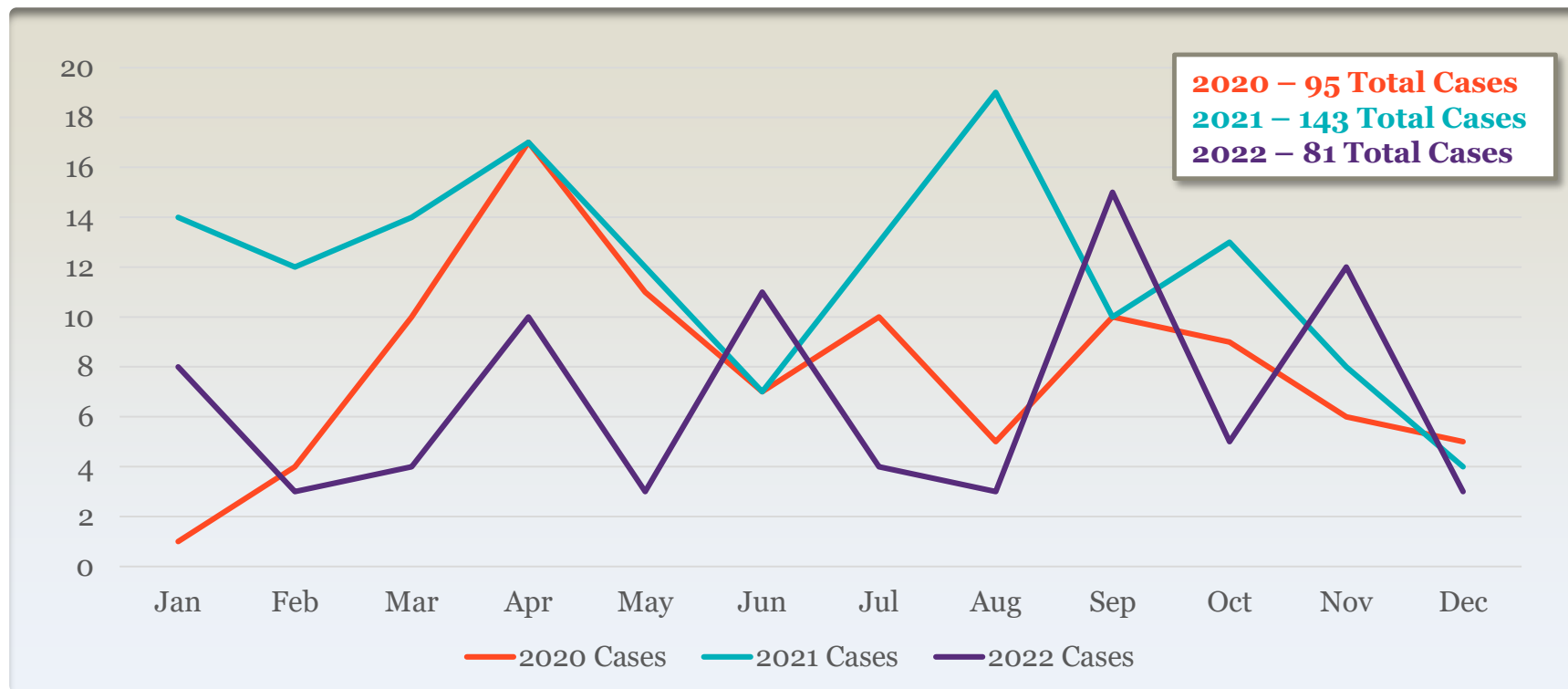
Proposed rules would require registered investment advisors and investment companies to implement specific written cybersecurity policies and procedures to address cybersecurity risks and to disclose cybersecurity risks/incidents affecting both advisers and funds along with their clients and stakeholders.



CCPA Private Right of Action

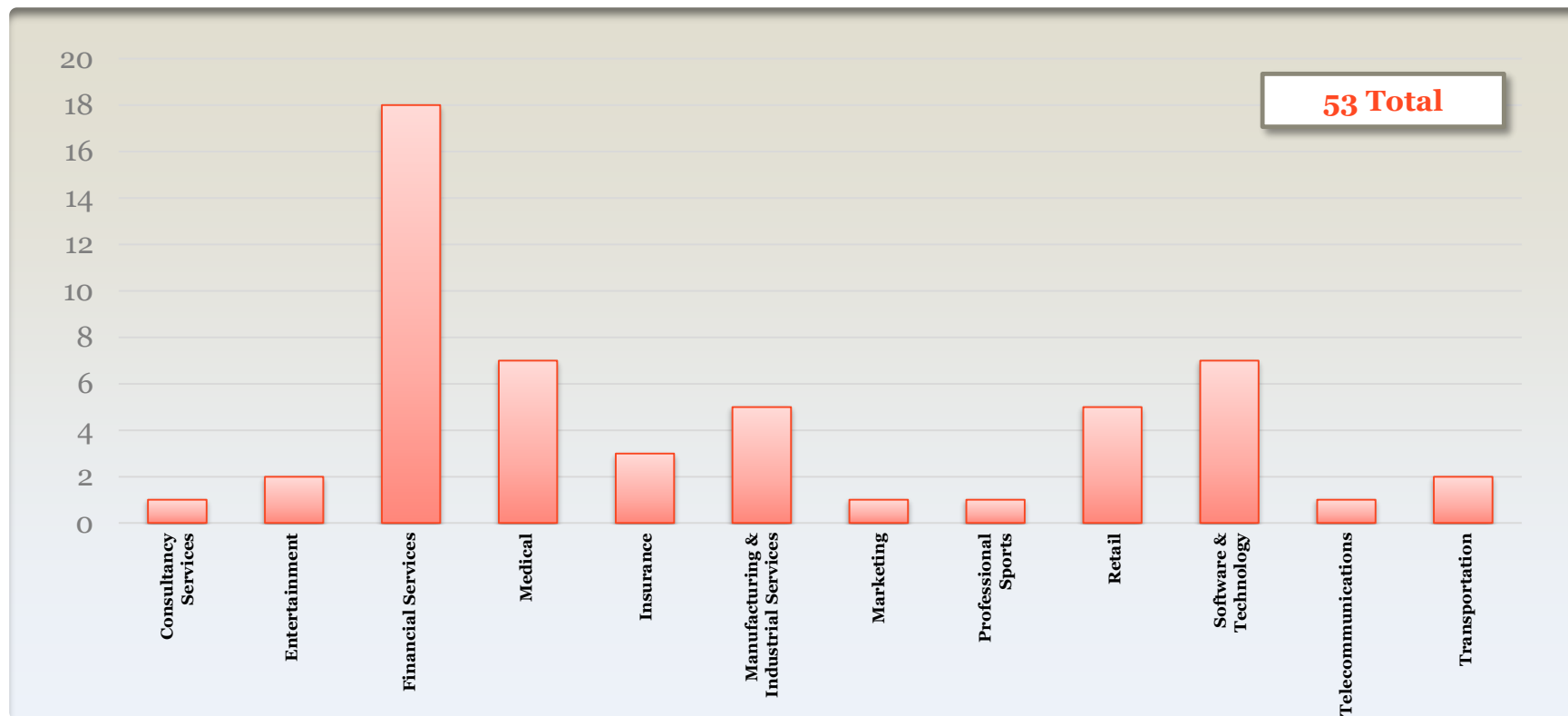


CCPA Cases Year Over Year: 2020 – 2022



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

Companies Facing CCPA Claims by Industry in 2022



Where Are CCPA Cases Being Filed?

- Since January 1, 2022, **51** cases have been filed in federal courts, and 30 cases in state court (through December 31, 2022)
- Total companies facing CCPA claims in 2022: **53**
- 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	21
Central District of California	12
State Superior Court, San Diego County	8
State Superior Court, San Francisco County	5

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

Takeaways

1. Plaintiffs are recognizing that the CCPA cannot serve as a predicate for other claims.
2. Federal courts are likely to find Article III standing where highly sensitive personal data is compromised.
3. California remains the top jurisdiction (both state and federal courts), but cases may be transferred to a defendant's principle place of business.
4. The financial services industry (banks, lenders, servicing companies) has been the primary target of consumers' 2022 CCPA-related suits, similar to last year.
5. No class involving a CCPA claim has been certified—and few cases are even reaching the class certification stage.
6. Executive officers face liability for security failures leading to CCPA claims.
7. Settlements are trending towards claims-made vs. lump sum.

International Data Protection



Executive Order and EU-US Adequacy

- **Biden Executive Order (EO)** – The European Commission (EC) previously launched the formal process to adopt the draft adequacy decision, which outlines its assessment of President Biden’s October EO and concludes that the order provides an adequate level of protection for personal data transferred from the EU to U.S. companies.
- On January 17, 2023, the European Data Protection Board (EDPB) discussed the draft adequacy decision for the proposed EU-U.S. Data Privacy Framework (DPF) (commonly referred to as “Privacy Shield 2.0”), featuring a presentation by European Commissioner for Justice Didier Reynders.
- In a non-binding opinion issued February 14, 2023, the European Parliament’s Committee on Civil Liberties, Justice and Home Affairs recommended that the EC reject the proposed EU-U.S. DPF.
- On February 28, 2023, the EDPB issued a non-binding opinion stating the DPF had made “substantial improvements” over the last Privacy Shield framework, but that additional clarity is needed.
- The EC will now consider the EDPB and the Committee’s opinions to decide whether to adopt the DPF Adequacy Decision.

EU Legislative Developments

Regulation on Artificial Intelligence (“AI Act”)

- The AI Act aims to address the risks generated by specific uses of AI through a set of harmonized rules.
- The goal is for a common regulatory and legal framework for all providers and users of AI systems that are on the EU market.
- The Act will have extraterritorial effect, is sector-agnostic, carries steep noncompliance penalties and applies to multiple stakeholders across the AI value chain, including users and providers.
- On December 6, 2022, the Council of the European Union (EU) adopted its amendments to the AI Act. The European Parliament must now finalize their common position before trilogues begin.
- The Act could enter into force by the end of 2023.

Digital Markets Act (DMA)

- The Digital Markets Act (DMA) entered into force on November 1, 2022. The DMA will start to apply starting on May 2, 2023.
- Within two months and at the latest by July 3, 2023, potential gatekeepers will have to notify their core platform services to the Commission if they meet the thresholds established by the DMA.
- Once the Commission has received the complete notification, it will have 45 working days to make an assessment as to whether the undertaking in question meets the thresholds and to designate them as gatekeepers (for the latest possible submission, this would be by September 6, 2023). Following their designation, gatekeepers will have six months to comply with the requirements in the DMA, at the latest by March 6, 2024.

Digital Services Act (DSA)

- The DSA’s purpose is to rebalance the rights and responsibilities of users, online intermediaries, online platforms and public authorities.
- The DSA’s EU-wide diligence obligations will apply to all digital services that connect consumers to goods, services or content.
- On October 4, 2022, the European Council gave its final approval to the Digital Services Act. It was published in the Official Journal of the European Union on October 19.
- Affected service providers will have until January 1, 2024, to comply with its provisions.

Other EU Legislative Developments

Data Governance Act

- The Data Governance Act seeks to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data.
- Entered into force on June 23, 2022, and, following a 15-month grace period, it will be applicable starting in September 2023.

Data Act

- The proposed law was published by the Commission on February 23, 2022. The Parliament and Council are defining their respective positions on the Data Act.

E-Privacy Regulation

- The E-Privacy Regulation is intended to update laws applicable to telecommunications as well as digital and online data processing.
- On January 5, 2021, the Portuguese Presidency released a new draft version of the proposed ePrivacy Regulation. On February 10, 2021, the member states agreed on a mandate for negotiations with the European Parliament and trilogues began on May 20, 2021.

AI Liability Directive

- On September 28, 2022, the Commission proposed a targeted harmonization of national liability rules for AI, making it easier for victims of AI-related damage to get compensation. It is likely to come into force late 2023/2024, with a two year grace period.

Digital Operational Resilience Act (DORA)

- On November 28, 2022, the European Council adopted 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 ICT (information communication technologies) related services to them, such as cloud platforms or data analytics services. DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats. These requirements are homogenous across all EU member states.
- DORA was published in the Official Journal of the European Union on December 27, 2022. It applies starting on January 17, 2025.

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 Parliament and the Council are examining the draft Act.

NIS2 Directive

- The Directive was published in the Official Journal of the European Union in December 2022. Member states must adopt and publish the measures necessary to comply with the NIS 2 Directive by October 17, 2024. The measures will apply starting on October 18, 2024.

United Kingdom Developments

- Online Safety Bill
 - 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.
 - The Bill is expected to return to the House of Lords this month (March 2023).
 - In November 2022, measures requiring the taking down of “legal but harmful” materials were removed from the Online Safety Bill.
 - The U.K. government is to propose an amendment introducing a criminal offense designed to capture instances where senior managers at technology companies, or those purporting to act in that capacity, have consented or connived in ignoring enforceable requirements, risking serious harm to children. The penalties will include fines and imprisonment.
- Network and Information Systems (NIS) Regulations
 - Came into force in 2018 to improve the cybersecurity of companies providing critical services. Organizations that fail to put in place effective cybersecurity measures can be fined as much as £17 million for noncompliance. On November 30, 2022, the government confirmed that the current (NIS) Regulations will be strengthened to protect essential and digital services against increasingly sophisticated and frequent cyberattacks.

United Kingdom Developments (Cont.)

- Product Security and Telecommunications Infrastructure Act of 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.
- 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.
 - It entered the legislative process in July 2022. Second reading of the Bill was postponed in September 2022 to allow ministers to consider the legislation further.
 - Will now be spearheaded by the U.K.'s newly minted Department for Science, Innovation and Technology (DSIT).

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 | • Bahrain | • Rwanda |
| • United Arab Emirates (UAE) | • Oman | • Uganda |
| • Brazil | • Thailand | • Ecuador |
| • Qatar | • Indonesia | • Russia |
| • Kuwait | • Botswana | • Belarus |
| • South Korea | • India | • 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 become enforceable six months following the issuance of executive regulations by the UAE Data Office, and no such regulations have as yet been issued.
- **Saudi Arabia:** 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:** In November 2022, the Ministry of Electronics and Information Technology of India introduced a draft of the Digital Personal Data Protection Bill 2022, although the bill has not yet been finalized.
- **Switzerland:** On August 31, 2022, the Swiss Federal Council adopted the revised Data Protection Ordinance and confirmed that the revised Federal Act on Data Protection and the Ordinance will enter 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 2022, among others:
 - For the **cross-border security assessment**, the Measures for the Security Assessment of Outbound Data Transfers and Guide to Applications for Security Assessment of Outbound Data Transfers (First Edition) were issued on July 07, 2022, and August 31, 2022.
 - For the **cross-border data transfer standard contract**, the draft Provisions on the Standard Contract for Outbound Cross-border Transfer of Personal Information also sought public comments in June and July 2022.
 - For the **security authentication/certification**, the Specification on Security Authentication for Cross-border Personal Information Processing Activities was initially issued in June 2022 and was updated to Version 2 later in December 2022.
 - For the **cybersecurity review**, the Measures for Cybersecurity Reviews, which was initially issued in April 2020, was updated in December 2021 and took effect on February 15, 2022. The revised rules include data processing activities of platform companies into the regulatory scope of the cybersecurity review system and require online platform operators that process more than 1 million users' personal information to pass cybersecurity review before offshore listing.

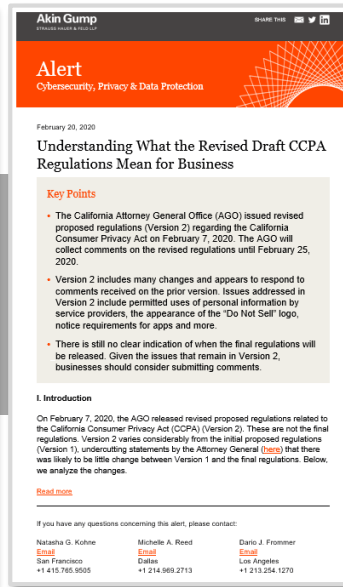
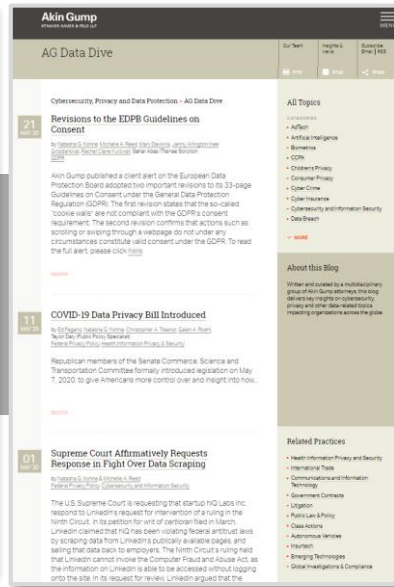
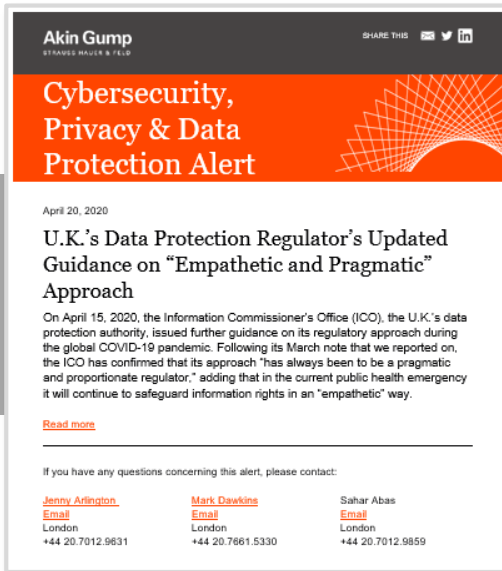




Takeaways

Akin Gump Resources

- Global and U.S. cybersecurity and privacy updates through Akin Gump's AG Data Dive Blog and client alerts.
- The latest edition of our annual CCPA Litigation Report will be released in the coming weeks! Please email any of the panelists to be notified when it is released.



Team Contact Information



Natasha Kohne, CIPP/US

Partner

Akin Gump Strauss Hauer & Feld LLP
San Francisco

T: 415.765.9505

nkohne@akingump.com



Michelle Reed, CIPP/US

Partner

Akin Gump Strauss Hauer & Feld LLP
Dallas

T: 949.885.4218

mreed@akingump.com



Molly E. Whitman

Counsel

Akin Gump Strauss Hauer & Feld LLP
Los Angeles

T: 310.728.3737

mwhitman@akingump.com



Mary Blatch

Senior Privacy Counsel
StockX



Anthony T. Pierce, Moderator

Partner

Akin Gump Strauss Hauer & Feld LLP
Washington, D.C.

T: 202.887.4411

apierce@akingump.com