



Data Privacy and Security Forum: 2021 Year in Review and What to Expect in 2022

Association of Corporate Counsel, National Capital Region – March 17, 2022

Natasha Kohne, Partner, Akin Gump

Michelle Reed, Partner, Akin Gump

Courtney Manzel, Corporate Counsel,
Privacy & Data Governance, Volkswagen
Group of America

Moderated by:
Tony Pierce, Partner, Akin Gump

AGENDA

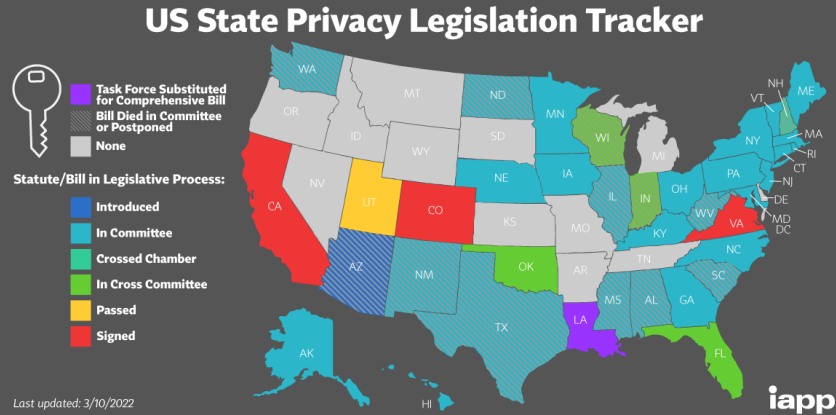
- State Privacy Updates
- California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
- Other State Privacy Updates
- Federal Agency Activity
- International Data Protection
- Adtech Updates
- CCPA Private Right of Action
- Takeaways



State Privacy Updates

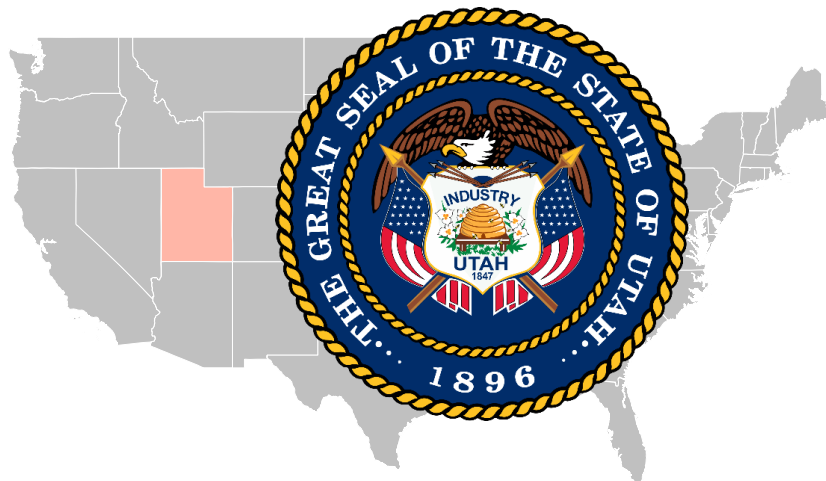
Evolving State Regulations

- Heading into 2022, **3** states have comprehensive privacy legislation and **25** states have had legislation introduced.
- All **50** states and U.S. territories have implemented data breach notification laws.
- **38** states introduced **160** consumer privacy-related bills in 2021, up from 30 in 2020.
- **15** states are introducing comprehensive consumer privacy legislation in 2022, including Washington, Florida, Minnesota and Connecticut.



Utah

- With the passage of the Utah Consumer Privacy Act (UCPA) this March, Utah has become the fourth and latest state to pass comprehensive data privacy legislation. The law takes effect December 31, 2023.
- The Utah Attorney General (AG) will be able to recommend changes via a report on the law's effectiveness, due July 1, 2025.
- Although not differing greatly from the Colorado Privacy Act (CPA) or the Virginia Consumer Data Protection Act (CDPA), the law is unique in some respects:
 1. Narrow applicability
 2. Limited right to delete
 3. No profiling opt-out
 4. Additional exception to "sale"
 5. No opt-in consent for sensitive data
 6. No data processing assessments
 7. No right to appeal
 8. No sunset for right to cure
 9. Enforcement



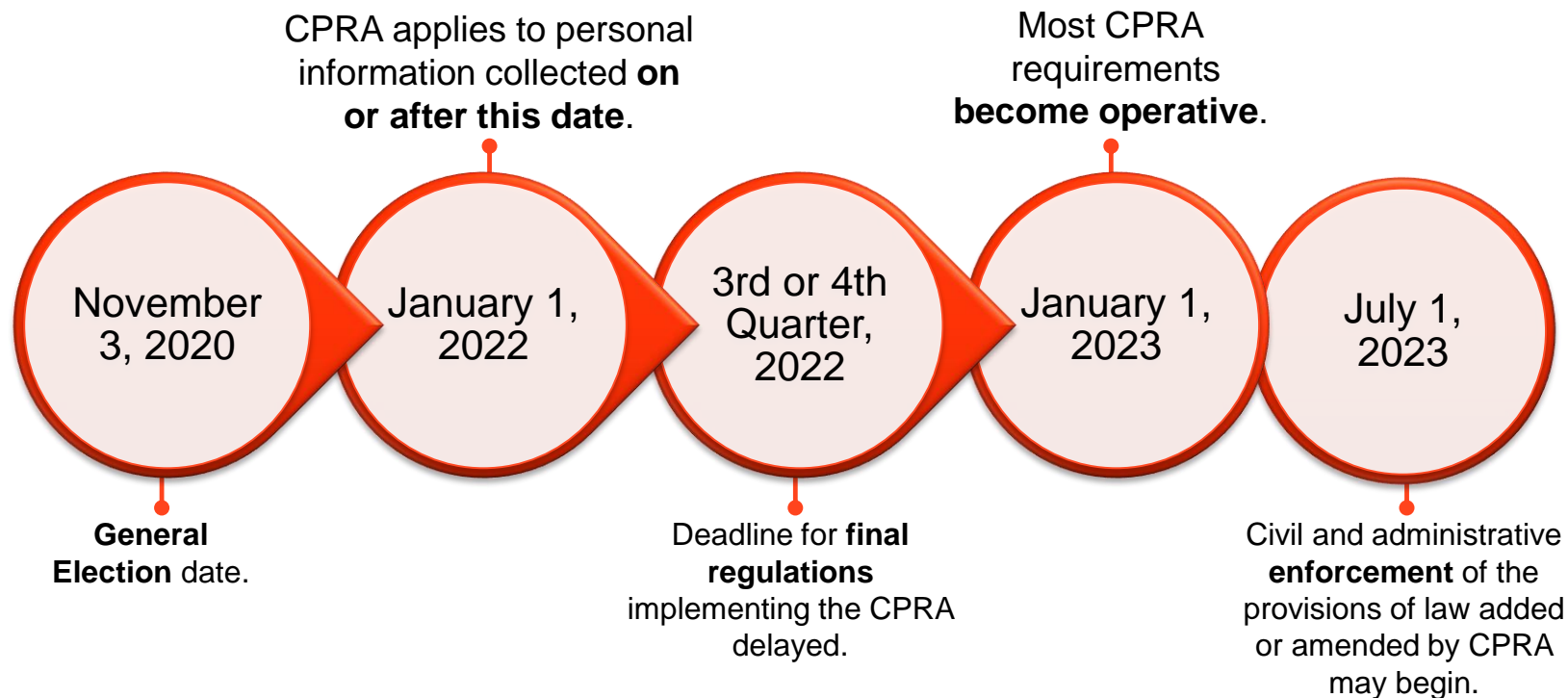
VA, CA, CO and UT Privacy Law Comparison

	Virginia Senate Bill 1392	California CPRA	Colorado Senate Bill 21-190	Utah Senate Bill 227
Scope of Application	<ul style="list-style-type: none"> Conducting business in Virginia or Produce products or services for Virginia residents and Process 100,000 consumers' data or process 25,000 consumers' data but derive over 50 percent of gross revenue from the sale of personal data. 	<ul style="list-style-type: none"> Conducting business in California and \$25M annual gross revenue or Buy, sell or share data of 100,000 consumers/households or 50 percent or more annual revenue from selling or sharing consumers' data. 	<ul style="list-style-type: none"> Conducting business in Colorado or Produce or delivers products/services targeted to Colorado residents, and Controls or processes 100,000 consumers' data or 25,000 consumers' data and derives revenue or receives discount from sale of data. 	<ul style="list-style-type: none"> Conducting business in Utah or Produce products/services targeted to Utah residents, and Have \$25M annual revenue, and Controls or processes 100,000 consumers' annually, or 50 percent or more gross revenue from sale of data and control or process data of 25,000 consumers.
Effective Date	January 1, 2023	January 1, 2023	July 1, 2023	December 31, 2023
Right to access	✓	✓	✓	✓
Right to correct inaccuracies	✓	✓	✓	✗
Right to delete	✓	✓	✓	✓
Right to opt out of targeted advertising or sale of personal data	✓	✓	✓	✗
Right to appeal	✓	✗	✓	✗
Time to respond to consumer requests	45 days from receipt of request. Extendable once for an additional 45 days	45 days from receipt of request. Extendable once for an additional 45 days	45 days from receipt of request. Extendable once for an additional 45 days	45 days from receipt of request. Extendable once for an additional 45 days
Obligations on controller to keep personal data secure	✓	✓	✓	✓
De-identified / pseudonymous data	✗	✗	✗	✗
Assessment required	✓	✗	✓	✗
Cure period before enforcement	30 days from issuance of a notice of violation	30 days from consumer written notice in cases of private right of action only	60 days from issuance of a notice of violation	30 days from issuance of a notice of violation
Private right of action	✗	✓	✗	✗
Attorney General enforcement maximum penalty	Up to \$7,500 per violation	\$2,500 per violation or \$7,500 per intentional violation or violations involving actual knowledge of data of consumers under 16	Up to \$20,000 per violation	Actual damages to consumer and up to \$7,500 per violation



California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

CPRA Key Dates



Top 10 Operational and Legal Considerations to Prepare for the CPRA

1. Refresh Data Map (e.g., sensitive personal information, B2B, employee, etc.)
2. Revise Service Provider and Contractor agreements
3. Enter into Third-Party agreements
4. Revise Data Retention Plan to identify the time period for which each category of PI is retained
5. Conduct regular Risk Assessments if processing of PI presents a significant risk to consumer's privacy or security
6. Conduct annual, independent Cybersecurity Audit if processing of PI presents significant risk to consumers' privacy or security
7. Update information security policies and practices and continue implementation of "reasonable security"
8. Revise Privacy Policy and Notice at Collection
9. Review Notice of Right to opt-out
10. Consider internal documentation (e.g., deletion record; training program, etc.)

GDPR vs. CCPA vs. CPRA

Components	GDPR	CCPA	CPRA
Right to Restrict Use of Your Sensitive Personal Information	✓	✗	✓
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	✗	✓

CCPA Enforcement

- Former California 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
- Once a company is notified, it currently has 30 days to cure
- The current California AG, Rob Bonta, posted a list of 27 examples of these enforcement actions, providing examples of curative actions
- Examples of noncompliance by the California AG include:
 1. Do Not Sell disclosures and implementation
 2. Service provider classification, contracts and compliance
 3. Application of CCPA exemptions
 4. Privacy Policy and Notice at Collection
 5. Access and deletion requests
 6. Financial incentives



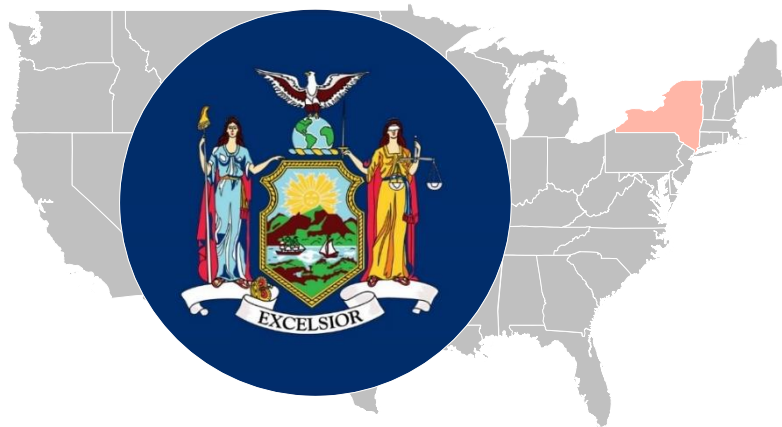
Xavier Becerra, Former California Attorney General



Other State Privacy Updates

New York Biometric Privacy Law

- New York City Council Bill 1170-2018 was enacted on January 10, 2021
- Went into effect on July 9, 2021
- Requires businesses to notify customers of the use of biometric identifier technology and prohibits the sale of biometric identifier information
- Addresses the increased collection and use of biometric identifier information by commercial establishments to track consumer activity, as well as:
 - Prohibits the sale of biometric identifier information
 - Requires certain commercial establishments, such as retailers, restaurants and entertainment venues, to post signage notifying consumers if they collect biometric identifier information
 - Provides for a private right of action allowing for judgments of \$500 for failures to post signage or negligently selling/sharing biometric information, and \$5,000 for the intentional or reckless sale of biometric information



Recent Biometric Privacy Developments

- Biometrics continue to be added to state data breach notification laws
 - Including TX, NY, CA, WA, AK
- Continued trend of class action lawsuits stemming from Illinois' Biometric Information Privacy Act (BIPA)
- Increased scrutiny from regulators could lead to larger fines
- Biometric litigation: Texas suit against Meta for alleged violations of state's biometric privacy law (February 14, 2022)



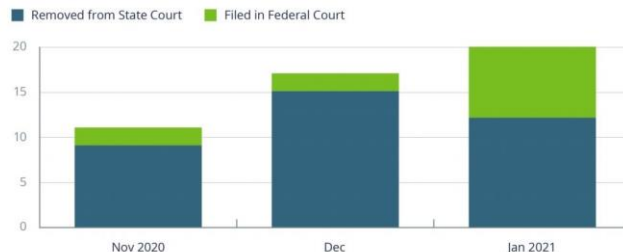
Portfolio Media, Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 |
www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Facebook, Ill. Users Ink Record \$550M Biometric Privacy Deal

By Allison Grande

Law360 (January 29, 2020, 10:52 PM EST) -- Facebook has agreed to pay a record \$550 million to resolve a biometric privacy class action pressed by Illinois users, putting an end to a dispute that was on the verge of a trial in California federal court that could have led to billions of dollars in damages.

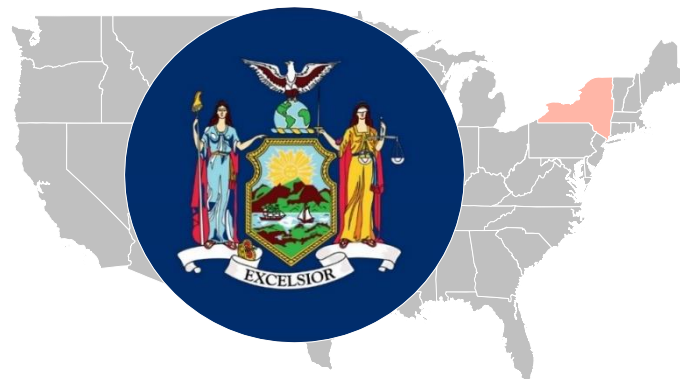
Most Pending Federal BIPA Actions Were Removed from State Court November 2020 through January 2021



Source: Bloomberg Law Dockets keyword search and analysis of BIPA complaints and Notices of Removal November 2020 through January 2021

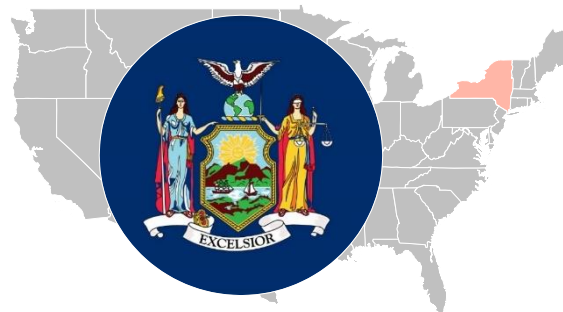
New York AI Law

- New York City Council Bill 1894-2020 was enacted on November 10, 2021
- Going into effect January 2, 2023
- Restricts the use by employers and employment agencies of artificial intelligence and machine-learning tools in hiring and promotion decisions
- The scope is broad, encompassing automated employment decision tools defined as “any computational process, derived from machine learning, statistical modeling, data analytics or artificial intelligence” that generates a “simplified output.”
- The law requires:
 - Notification to candidates 10 days in advance
 - An annual bias audit of the tool
 - Publishing of the bias audit on employer’s website



New York

- New York law governing electronic monitoring of employees (Senate Bill S2628), effective this May (November 2021).
- New York Department of Financial Services (NYDFS) 2021 Cybersecurity Regulation Enforcement Actions:
 - Residual Mortgage Services (March 2021): \$1.5 million fine
 - National Securities Corp. (April 2021): \$3 million fine
- Stop Hacks and Improve Electronic Data Security (SHIELD) Act (July 2019)
 - Filters Fast (May 2021): aggressive cyber regulation, extensive questions from the AG
 - EyeMed (February 2022): indicates remedial measures companies should take to comply with SHIELD
- NY Attorney General released guidance for businesses on stopping Credential-Stuffing attacks (January 2022)
- Senate Bill S567 (2020)
 - Comparable to CCPA; includes a private right of action
 - Referred to Consumer Protection Committee in 2022
- New York Privacy Act (A.B. A680) (2021)
 - Includes a consent requirement like that of the GDPR
 - Referred to Assembly Committee in 2022



State Data Breach Notification Updates

Approximately 22 states introduced or considered measures amending their existing security breach laws, with several bills enacted in 2021:

Imposed notice requirements on state entities

- Arkansas



Broadened existing definition of “personal information”

- California
- Mississippi



Incentivized businesses to have reasonable information security at time of breach

- Connecticut
- Utah



Required government entities to report data breaches to central state office of information technology

- New York
- Georgia
- North Dakota



Shortened timelines to notify

- Connecticut





Federal Agency Activity



Federal Trade Commission (FTC)

- Recently 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 conducted over 20 enforcement actions related to privacy and cybersecurity in the past two years. Most recently:
 - Ascension Data & Analytics, LLC, In the Matter of (December 22, 2021)
 - OpenX Technologies, Inc. (December 15, 2021)
 - Kuuhuub, Inc., et al., U.S. v. (Recolor Oy) (July 21, 2021)
 - Flo Health, Inc. (June 22, 2021)
 - Everalbum, Inc., In the Matter of (May 7, 2021)
 - Support King, LLC (SpyFone.com), In the Matter of (May 3, 2021)
 - Vivint Smart Home, Inc. (April 29, 2021)



Federal Data Privacy and Security Updates

- Congress has just passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022, as part of the omnibus spending package for FY 2022
 - Critical infrastructure providers in areas such as financial services and information technology will have a 72-hour reporting requirement for cyber incidents
- March 11, 2022—SEC proposes cybersecurity rules for public companies
- March 9, 2022—the White House issues an Executive Order on the need to address the role of digital assets and calling for federal action plans
- February 9, 2022—SEC proposes cybersecurity rules for registered investment advisors and funds
- January 6, 2022—the Securities and Exchange Commission (SEC) proposed rules that would affect digital asset trading platforms by expanding the definition of “exchange,” requiring platforms to comply with exchange-related requirements that would otherwise fit an exemption
- November 18, 2021—banking organizations and bank service providers will have a 36-hour cybersecurity breach notification requirement for cyber incidents that rise to the level of “notification events.” Effective April 2022.
 - Final Rule issued by the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (Board) and the Office of the Comptroller of the Currency (OCC)
- November 8, 2021—the U.S. Department of the Treasury Financial Crimes Enforcement Network (FIN-CEN) issued an updated version of its ransomware advisory release in fall 2020
- October 13, 2021—the White House issued a Fact Sheet with updates on the federal effort to counter ransomware, including agency actions against ransomware actors and infrastructure
- October 6, 2021—the DOJ launched its Civil Cyber-Fraud Initiative, focusing on fraud cases dealing with cybersecurity under the False Claims Act (FCA)
- September 21, 2021—the Treasury Department’s Office of Foreign Assets Control (OFAC) issued an updated advisory on sanctions compliance related to ransomware payments, emphasizing the importance of defense over paying ransoms
- August 11, 2021—the Federal Finance Institutions Examination Council (FFIEC) issued guidance establishing risk management principles and practices to support the authentication of users accessing a financial institution's information systems and customers accessing a financial institution's digital banking

Children's Privacy

- The Biden administration announced the need to strengthen children's privacy protections, particularly as related to social media, in the State of the Union Address
 - The remarks called for a ban on tech companies collecting children's data and targeted advertising to children
- In 2019, the FTC solicited comments as part of its review of the COPPA Rule
- The FTC has repeatedly included children's privacy in its list of priorities and initiated several related enforcement actions in 2021 and 2022:
 - Kuuhuub, Inc. – In July 2021, the FTC reached a \$1 million settlement with operators of an online coloring book app related to allegations of violations of the COPPA Rule
 - OpenX Technologies, Inc. – In December 2021, the FTC announced that the advertising platform will pay \$2 million to settle allegations that it collected personal information from children under 13 without parental consent and continued to collect geolocation data even after users had affirmatively opted out
 - Weight Watchers – In March 2022, the FTC reached a \$1.5 million settlement over allegations that Weight Watchers marketed a weight loss app for use by children as young as eight and then collected their personal information without parental permission. The settlement requires Weight Watchers to delete personal information illegally collected from children under 13 and destroy any algorithms derived from the data
- Industry watchdog groups are also monitoring companies' privacy practices affecting children
 - The Children's Advertising Review Unit announced this month that TickTalk, a smartwatch maker for kids, had submitted a plan to address CARU's findings that the company's notice and consent practices did not comply with COPPA
 - The self-regulatory program operated by CARU was the first of the six FTC-approved COPPA Safe Harbor Programs

International Data Protection

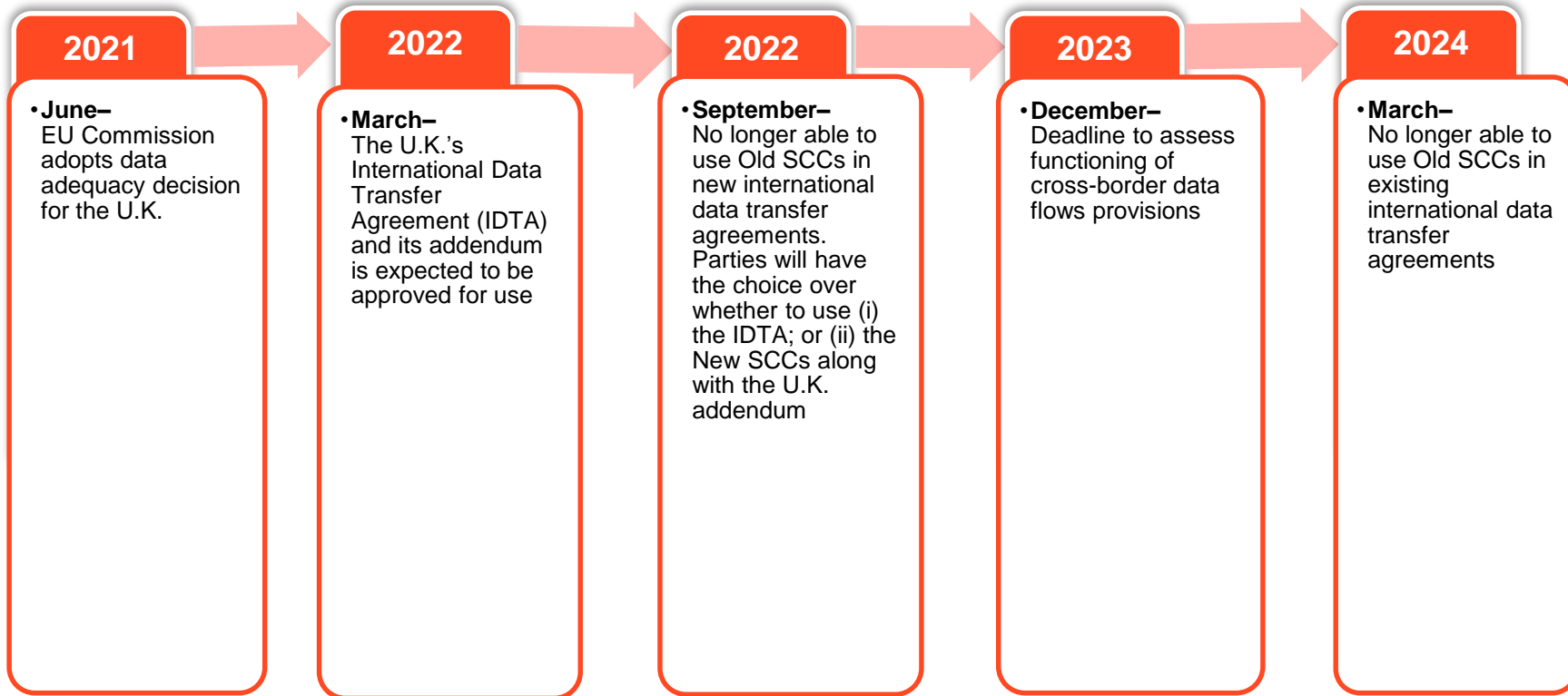


New SCCs

- As of September 27, 2021, all new contracts that seek to rely on Standard Contractual Clauses (SCCs) to make cross-border data transfers must incorporate updated SCCs (New SCCs)
- New SCCs impose more onerous obligations on importers and exporters of personal data from European Economic Area (EEA)
- More than 2 parties may now adhere to the same set of SCCs. All parties must conduct a transfer impact assessment to assess whether the laws and practices of the data importer's country and practice of the data importer's country pose a barrier to the parties' compliance with the New SCCs
- Contracts based on Old SCCs may be relied upon until **December 27, 2022**, by which time businesses must have transitioned to New SCCs

Data Transfer	Old SCCs	New SCCs
Controller to Processor	✓	✓
Controller to Controller	✓	✓
Processor to Controller		✓
Processor to Processor		✓

Brexit Update



Anticipated EU developments

E- Privacy Regulation

- The E-Privacy Regulation is intended to update laws applicable to telecommunications, as well as digital and online data processing
- Negotiations between EU Parliament and EU Commission for finalization of the Regulation continue. The e-Privacy Regulation is anticipated to be adopted in either 2022 or 2023, meaning that it will likely not come into effect until 2023 at the earliest

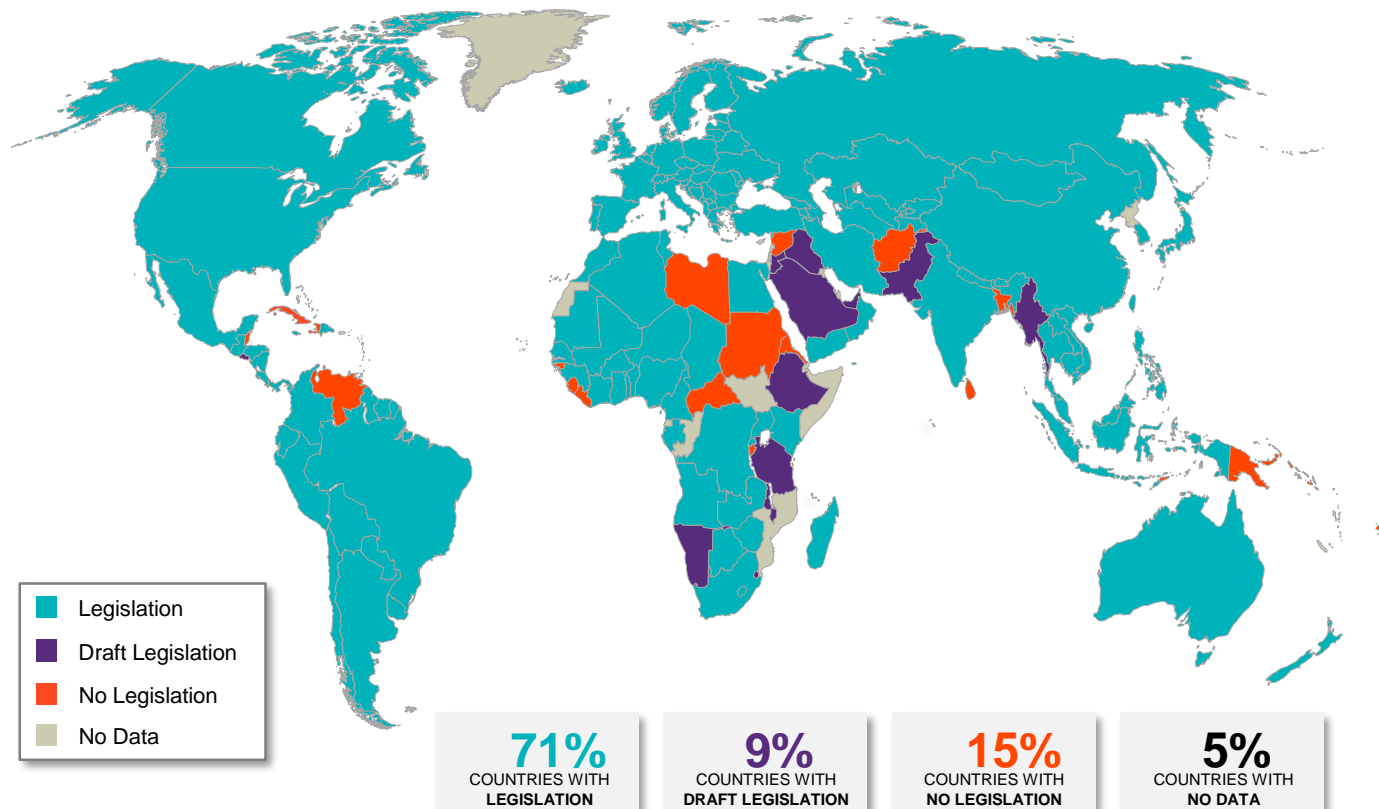
The European Commission's Artificial Intelligence Act (Act on AI)

- The Act on AI aims to address the risks generated by specific uses of AI through a set of harmonized rules. The Act will have extra territorial effect, is sector-agnostic, carries steep noncompliance penalties and applies to multiple stakeholders across the AI value chain, including users and providers
- The draft Act on AI, is currently going through the legislative procedure of the European Parliament and Council

Digital Markets Act (DMA)

- The DMA seeks to address the negative consequences arising from platforms acting as digital “gatekeepers” to the internal market by setting out harmonized rules defining and prohibiting unfair practices
- The DMA is not expected to enter into force until mid-2022, and is expected to have a transitional period of at least two months

Regulators Around the World



Major Legislative Developments Around the World in 2021

Significant new data privacy regimes on the rise globally—China, the UAE, Brazil, Russia and Switzerland, among others, passed new laws, amendments or implementing regulations

- **China:** On August 20, 2021, the Standing Committee of China's National People's Congress passed the Personal Information Protection Law (**PIPL**), which took effect on November 1, 2021
- **United Arab Emirates:** On November 27, 2021, the United Arab Emirates 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
- **Brazil:** During 2021, the Brazilian data protection authority (**ANPD**) adopted and published a series of guidance and FAQs regarding the LGPD, especially concerning guidance for data processing agents and officers, sanction and fines, the inspection process, and data subject rights
- **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 shall become effective on March 23, 2022
- **Switzerland:** On March 5, 2021, the Federal Data Protection and Information Commissioner (**FDPIC**) published guidance for both the private sector and federal authorities on adapting processing activities to comply with the transparency, portability, cross border transfer, and processing requirements of the revised Federal Act on Data Protection 1992 ("**Revised FADP**")
- **South Korea:** On December 17, 2021, the European Commissioner for Justice formally announced an adequacy decision between South Korea and the EU for transfers of personal data.
- **United Arab Emirates:** On September 20, 2021, the UAE issued Federal Law No. 34 of 2021, repealing the previous Cybercrimes Law (**Federal Law No. 5** of 2012) and establishing a more robust and sophisticated legal regime, addressing both cybercrime related offences and the spreading of false information
- **Rwanda:** On December 10, 2021, Rwanda's National Cyber Security Authority (NCSA) issued a notice on the Personal Data Law detailing that registration with the NCSA as a data controller or data processor is required prior to processing personal data.
- **Russia:** Beginning March 27, 2021, Russia increased the amounts of administrative fines prescribed in the Code of Administrative Offenses against the Federal Law On Personal Data

The Three Pillars of China's Data Protection Framework


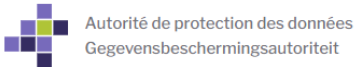

- **Personal Information Protection Law (PIPL) — November 1, 2021**
 - Applies to personal information processing entities (PIPEs), “an organization or individual that independently determines the purpose and means for processing of personal information.”
- **Data Security Law (DSL) — September 1, 2021**
 - Governs creation, use, transfer, storage or exploitation of data within China
- **Cybersecurity Law — June 1, 2017**
 - Defined security obligations of internet products and service providers, Increased data protection, data localization, and cybersecurity requirements.
- The Cybersecurity Law enabled the Chinese government to obtain any information deemed to have an impact on Chinese security from any person or entity in China. The DSL focuses on data security regulation while emphasizing safeguarding national security, and the PIPL focuses on the protection of personal information. The PIPL applies to organizations operating within China as well as foreign organizations processing information outside China, when processing personal information of persons in China in any of the following circumstances:
 1. The organization collects and processes personal information for purpose of providing products/services in China
 2. The data will be used in analyzing behavior of natural persons in China
 3. Other unspecified “circumstances stipulated by laws and administrative regulations.”



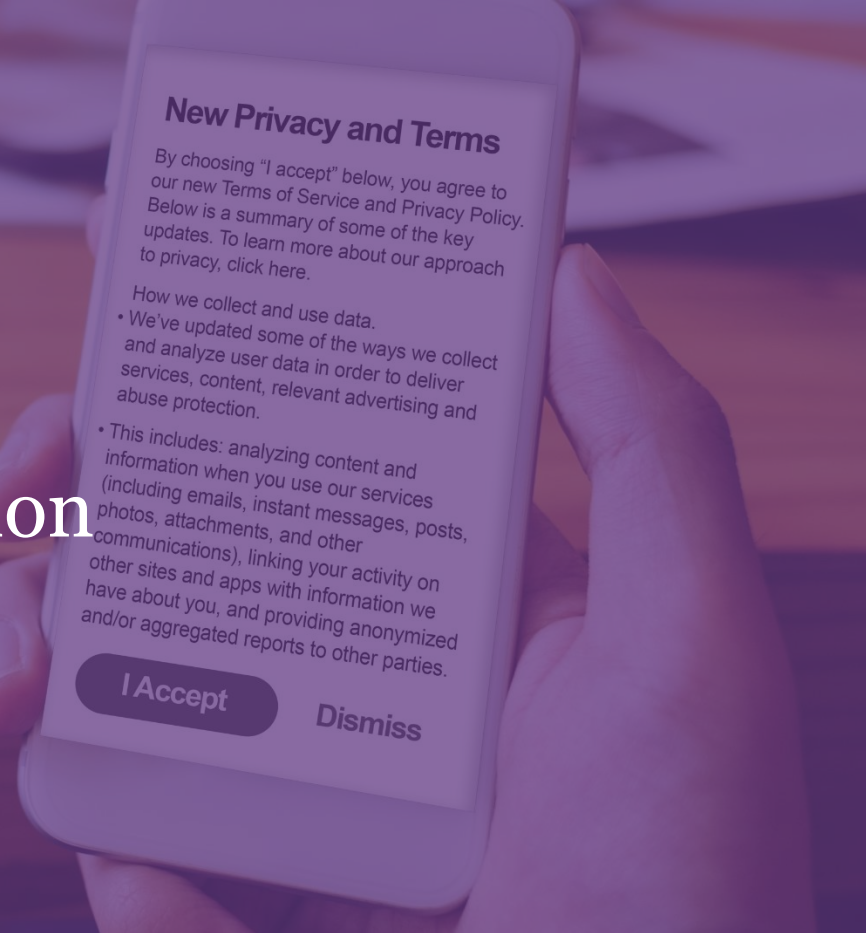


Adtech Updates

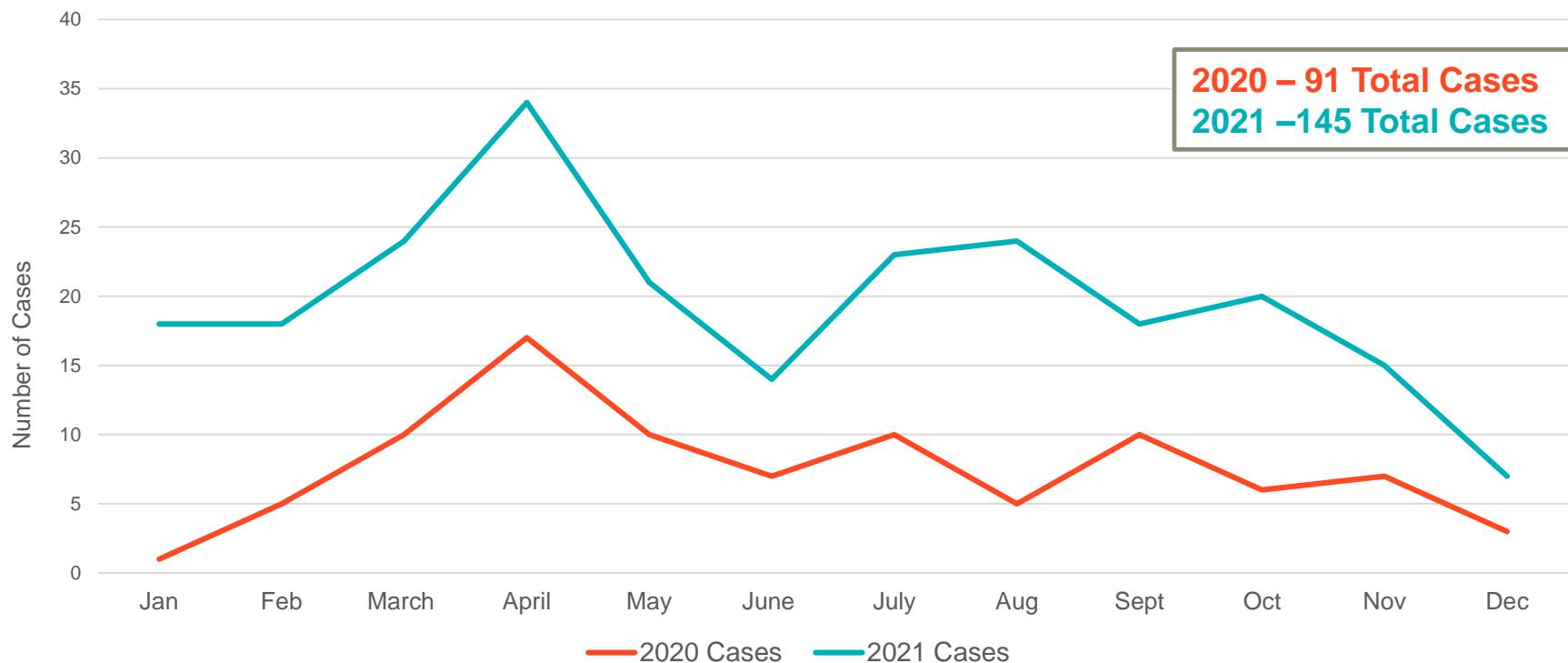
Adtech Updates – Key Developments

International	<ul style="list-style-type: none">• Enforcement Activities• Law and Regulations• Guidance	<p>Information Commissioner's Opinion: Data protection and privacy expectations for online advertising proposals</p>	 
U.S.	<ul style="list-style-type: none">• State Privacy Laws (CCPA, CPRA, CDPA and CPA)• FTC• Congress		 <p>FEDERAL TRADE COMMISSION PROTECTING AMERICA'S CONSUMERS</p>
Platform	<ul style="list-style-type: none">• Consumer Control• Increased Transparency• Movement Away from Third-Party Cookies		

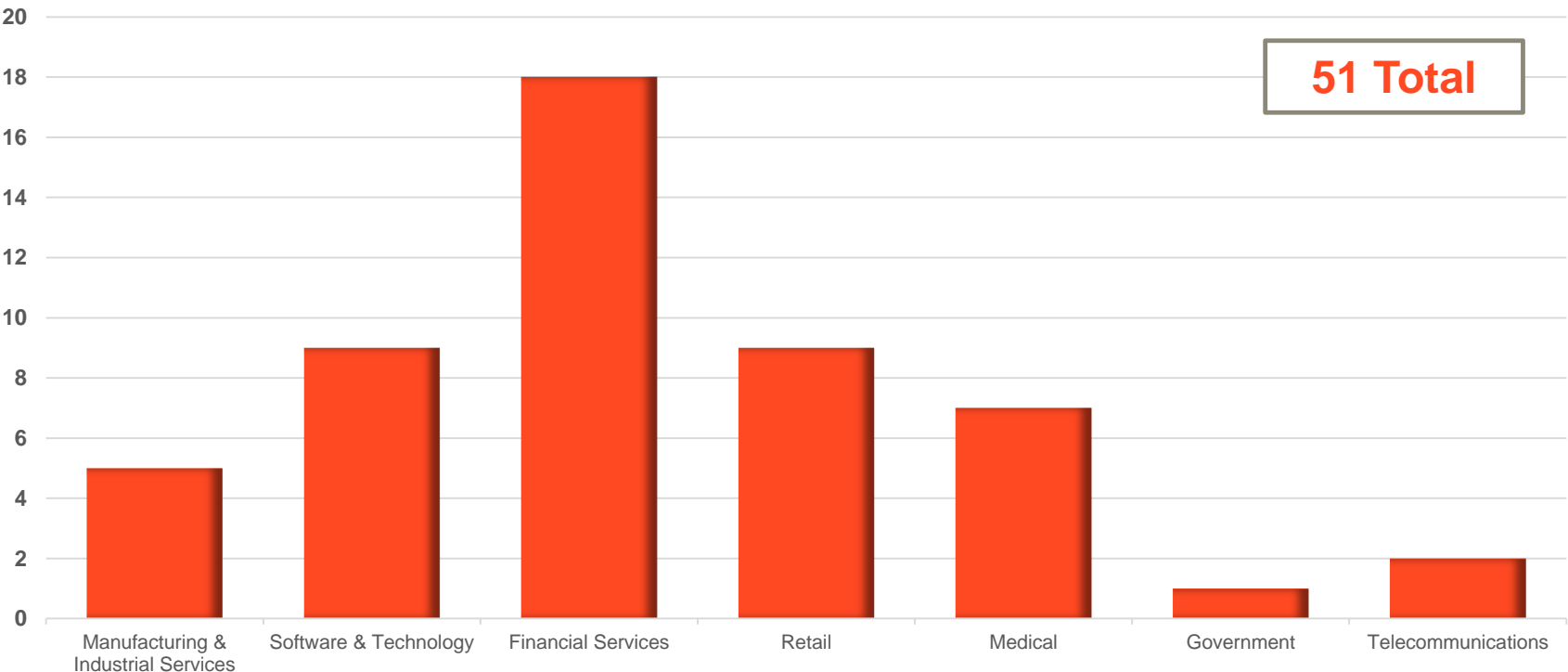
CCPA Private Right of Action



CCPA Cases Filed in 2020 vs. 2021



Number of CCPA Cases Across Industry Types (Based on unique defendants)



Where are CCPA Cases Being Filed?

- Since January 1, 2021, **102** cases have been filed in federal courts, and **43** cases in state court (through December 31, 2021)
- Total Unique defendants: **51**
- The majority of cases that cite to the CCPA have been filed in CA courts, but cases have also been filed in MO and IL



Top Courts

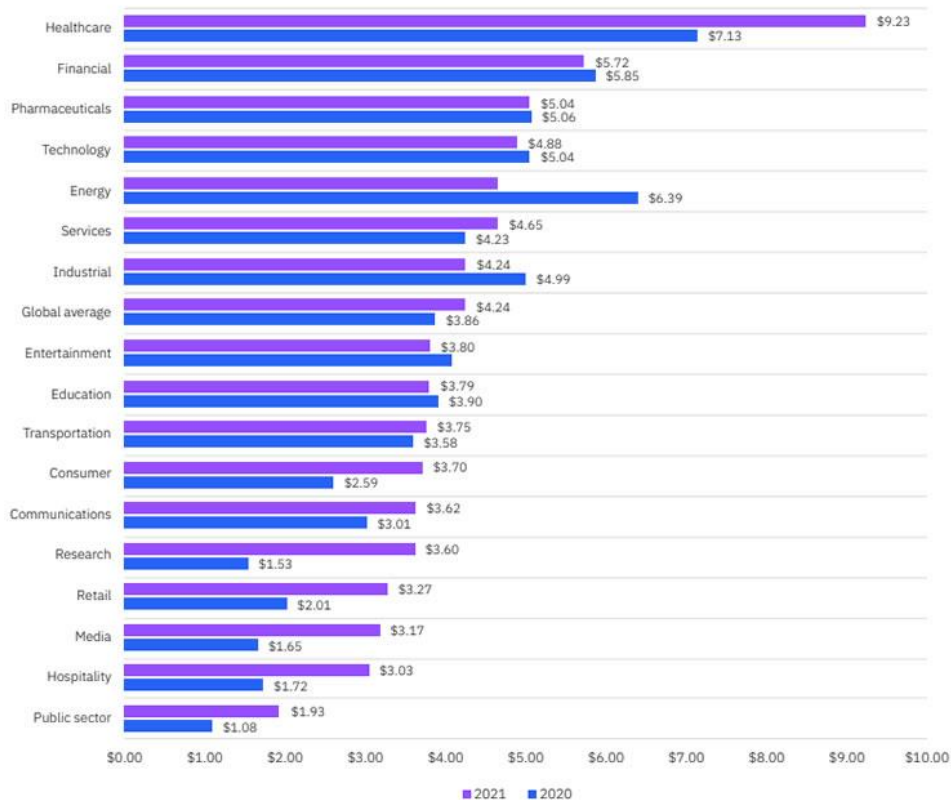
Court	Cases
Northern District of California	26
Central District of California	11
State Superior Court	40
Southern District of California	18

Data Breach Trends

- The number of data breaches in 2021 saw approximately a **50% increase**
- While exact litigation stats are difficult to come by, data breach litigation also continues to rise
- Data breaches continue to affect a wide range of industries
- As cases increase, plaintiff lawyers continue to rely on common cases of action
- Inaccurate information with no dissemination to third party is not concrete harm (*Ramirez v. Transunion*)
- Clark Hill case– Forensic reports may no longer be privileged (cited Capital One case)

Average total cost of a data breach by industry

Measured in US\$ millions



Takeaways

1. Traditional Data Breaches Dominated the 2021 CCPA Landscape
2. Plaintiffs Are Recognizing that the CCPA Cannot Serve as a Predicate for Other Claims
3. To Date, CCPA Claims Most Often Accompany Causes of Action for Negligence, California Unfair Competition Law, and Breach of Implied Contract
4. Federal Court Remains the Most Common Venue for CCPA Claims, but Ramirez May Change That Going Forward
5. CCPA Claims Have Been Brought in States Across the Country
6. All Sorts of Businesses from Software Companies to Banks and Manufacturers have Been Named as Defendants in CCPA Cases
7. Businesses May Face Liability For Third-Party Vendor's Breaches
8. Service Providers Beware: CCPA May Not Exempt You from Data Breach Liability
9. No Class Involving a CCPA Claim Has Been Certified—and Few Cases Are Even Reaching the Class Certification Stage
10. Settlements Are Trending Towards Claims-Made vs. Lump Sum



Takeaways

Top Privacy Concerns for Management

Increased Civil Litigation Risk

Third-Party Risk Management

Evolving Regulatory International, National and State Privacy Landscape

Rise in Cyber Insurance Premiums

Increased Scrutiny on Children's Data, Facial Recognition, Other Sensitive Data and AI

Cross-Border Transfers and GDPR Enforcement

The Coming Year+

More State Privacy Bills – What will pass, and who will be next?

Children's Data and COPPA

Tracking Technologies – Developments in digital advertising

Inter-agency and Inter-governmental cooperation – federal, state and international

Federal Rulemaking and Over-reporting of cyber incidents – SEC, CISA, etc.

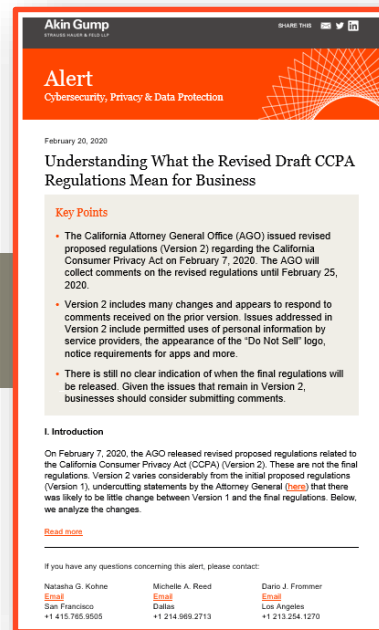
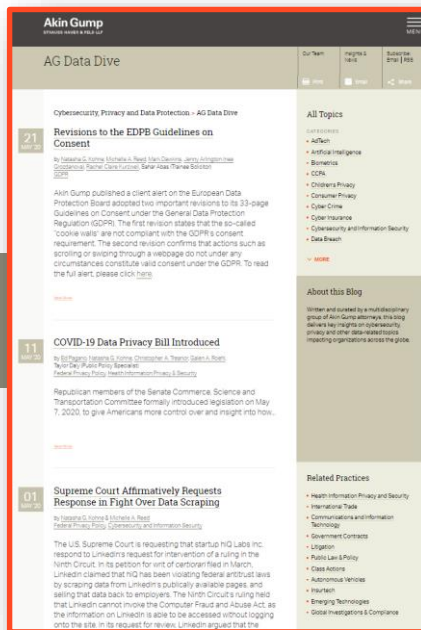
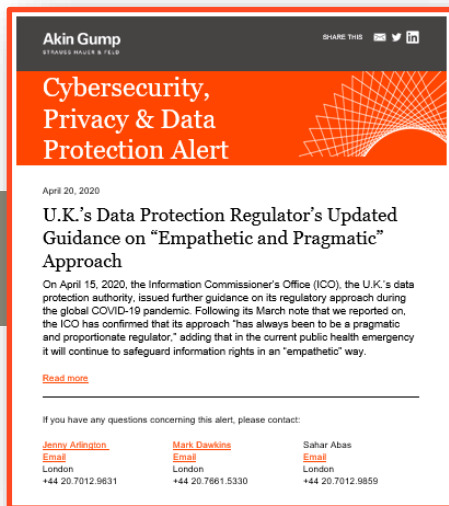
Facial Recognition/Biometrics – Expanding legislation and expensive litigation

Future of Cross-Border Data Transfers

Unregulated Emerging Technologies – AI, fintech, medtech, etc.

Akin Gump Resources

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



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



Courtney Manzel

Corporate Counsel, Privacy & Data Governance,
Volkswagen Group of America



Anthony T. Pierce

Partner, Akin Gump Strauss Hauer & Feld LLP

Washington, D.C.

T: 202.887.4411

apierce@akingump.com