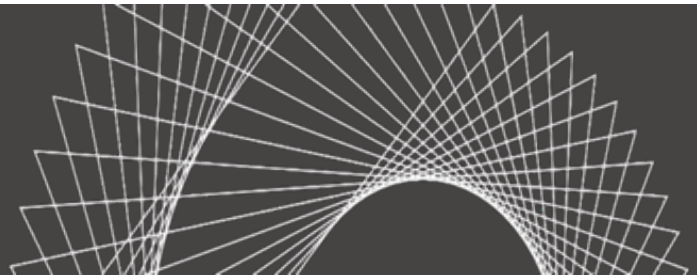
Data Privacy and Security Forum: 2020 Year in Review and What to Expect in 2021



Akin Gump
STRAUSS HAUER & FELD LLP

Association of Corporate Counsel, National Capital Region – February 23, 2021

Natasha Kohne, Partner, Akin Gump

Michelle Reed, Partner, Akin Gump

Amy Purcell, Chief Privacy Officer, Senior Counsel, Vanguard

Moderated by: Tony Pierce, Partner, Akin Gump

COVID-19

COVID-19

PRESIDENT JOSEPH R. BIDEN, JR.

NATIONAL STRATEGY FOR THE COVID-19 RESPONSE AND PANDEMIC PREPAREDNESS

JANUARY 2021

America Is Reopening. Coronavirus Tracing Apps Aren't Ready.

Smartphone apps meant to track where people have traveled or whom they have been near are mostly buggy, little-used or not ready for major rollouts, raising concerns as restrictions lift and infections rise

Interim Guidance for Businesses and Employers Responding to Coronavirus Disease 2019 (COVID-19), May 2020

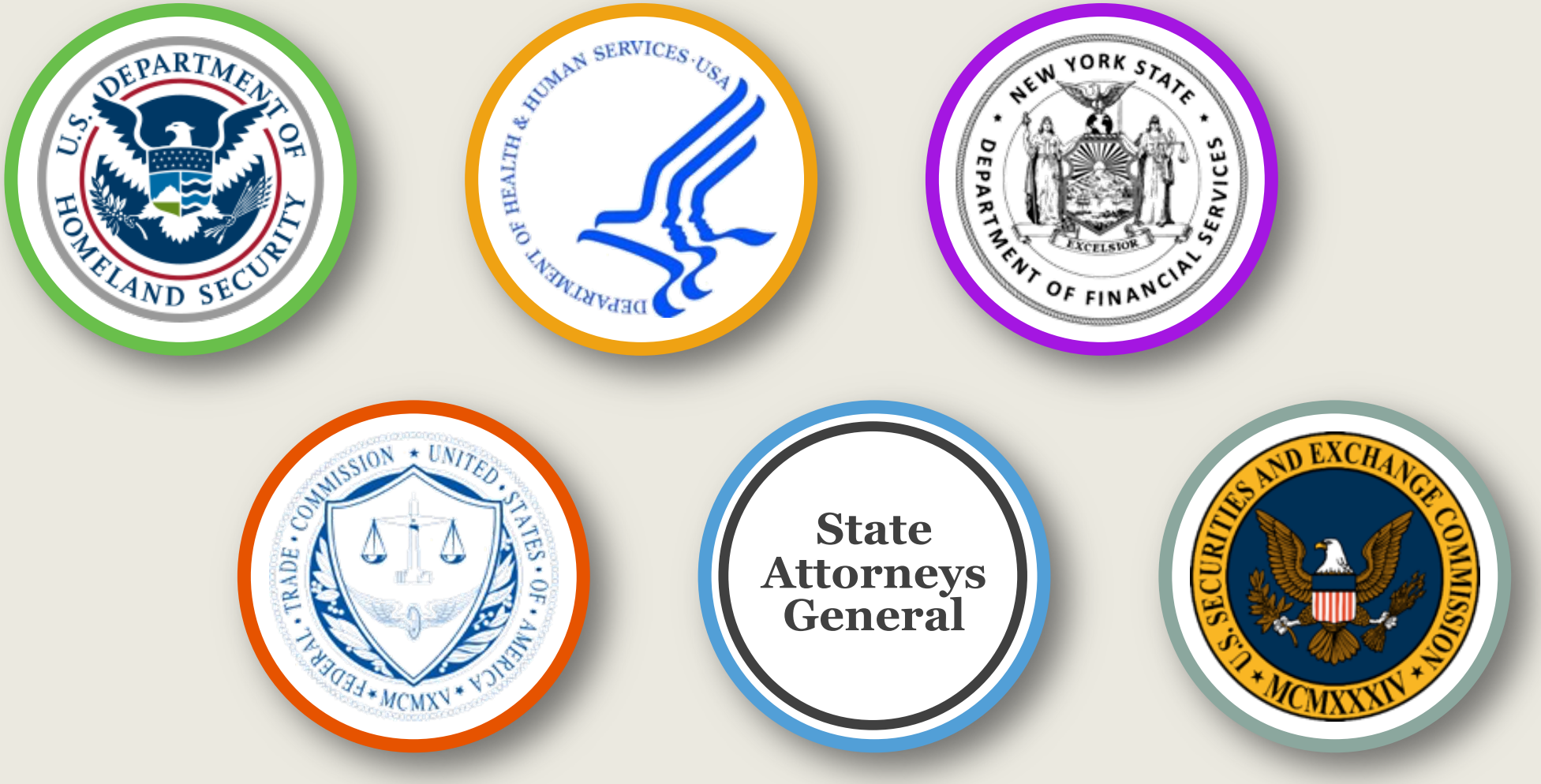
Plan, Prepare and Respond to Coronavirus Disease 2019

City and County of San Francisco Health Officer Directive - Attachment

Handout for Personnel (Employees, Contractors, Volunteers) of Essential Business and Other Businesses Permitted to Operate During the Health Emergency *(May 18, 2020)*

What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws

Regulators Warn of Cyber/Privacy Risks in Pandemic



GDPR and European Guidance During in COVID

Contact Tracing

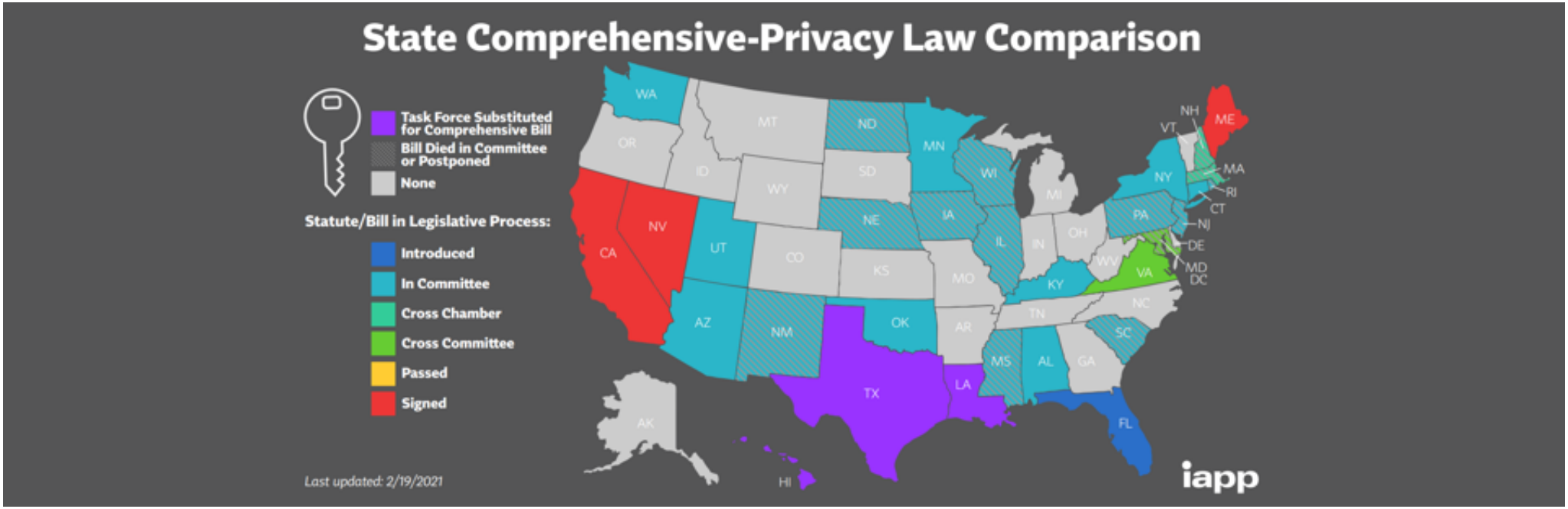
Employee Monitoring

Temperature Screening

State Privacy Updates

Evolving State Regulations

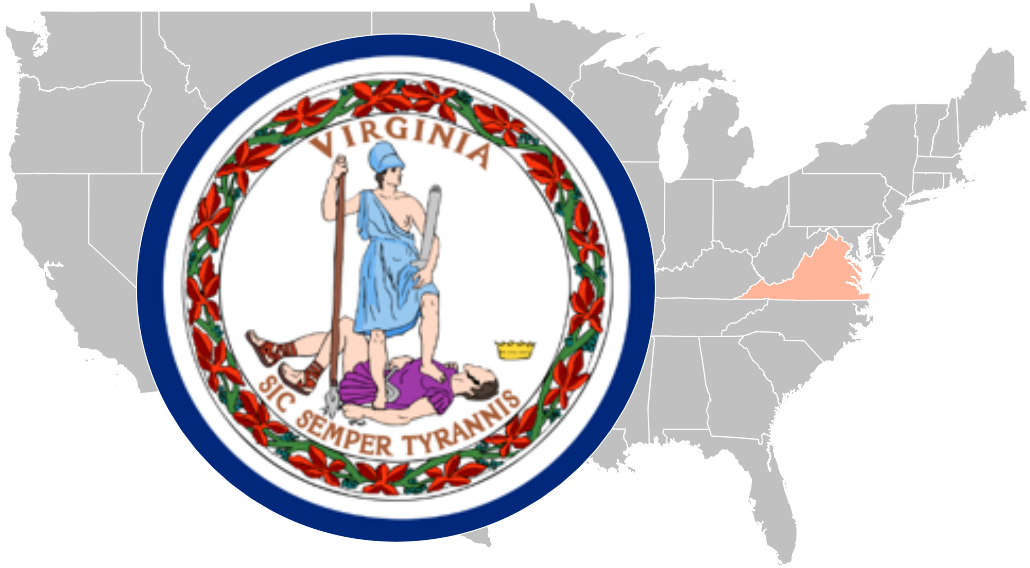
- As of February 19, 2021, **3** states have implemented unique privacy laws, **3** states have created taskforces and **25** states have had legislation introduced.
- All **50** states and U.S. territories have implemented data breach notification laws.
- Over **10** new state laws in the last two years expanded data breach obligations.
- **100%** of workplaces and homes have been transformed by COVID-19 and this has changed the privacy landscape.



Virginia

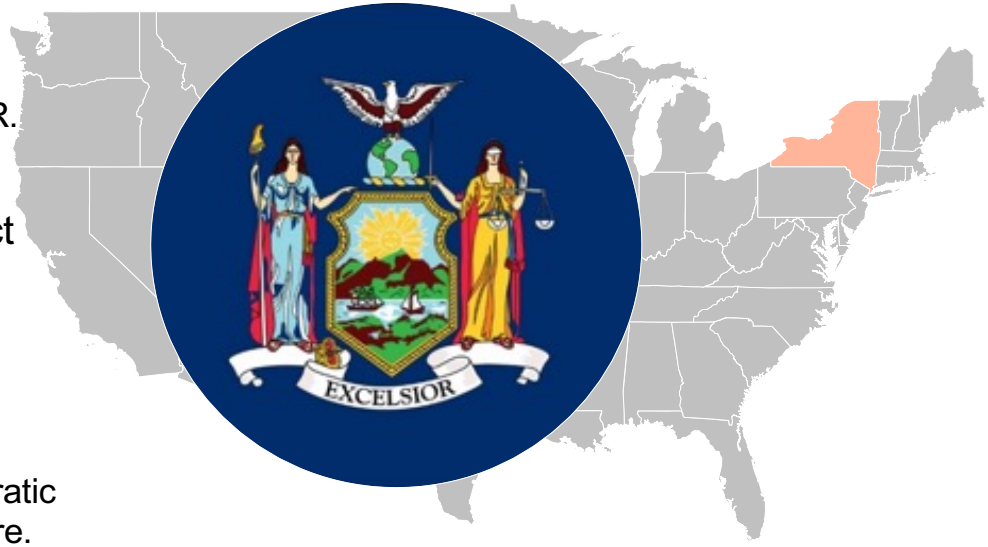
- The Virginia Consumer Data Protection Act (CDPA) passed the Virginia Senate on February 3, and has moved to the governor's desk later this month.
- If passed into law, the legislation would take effect in January 1, 2023.
- Tech industry trade groups, in addition to Amazon and Microsoft, have backed the bill.
- Borrows principles from the California Privacy Rights Act (CPRA), the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) but also differs from in key respects:

1. Applicability
2. Exemptions
3. Controller/processer distinction
4. Broad definition of personal data
5. Inclusion of sensitive data category
6. Individual rights
7. Data protection assessments
8. Enforcement



New York

- New York Department of Financial Services (NYDFS) Cybersecurity Regulation (March 2017)
  - Mandates minimum cybersecurity standards for any banking, insurance and brokerage firm using a license to operate in New York and requires covered entities to annually prepare and submit a certification of compliance with the NYDFS.
  - Certification of compliance with each provision was due for the first time by June 1, 2020, a deadline extended due to COVID-19.
- Stop Hacks and Improve Electronic Data Security (SHIELD) Act (July 2019)
  - Expands existing data breach notification requirements and puts into place new data security obligations on businesses that own, license or maintain computerized data that includes any NY resident's private information.
- Senate Bill S567
  - Comparable to the CCPA; includes a private right of action.
- New York Privacy Act (A.B. A680)
  - Includes a consent requirement like that of the GDPR.
  - Earliest it could become law is summer/fall 2021.
- New York Data Accountability and Transparency Act
  - Proposed in Gov. Cuomo's 2022 budget and would establish a Consumer Data Privacy.
- Bill of Rights
  - Could quickly gain traction, as there are now Democratic supermajorities in both houses of the state Legislature.

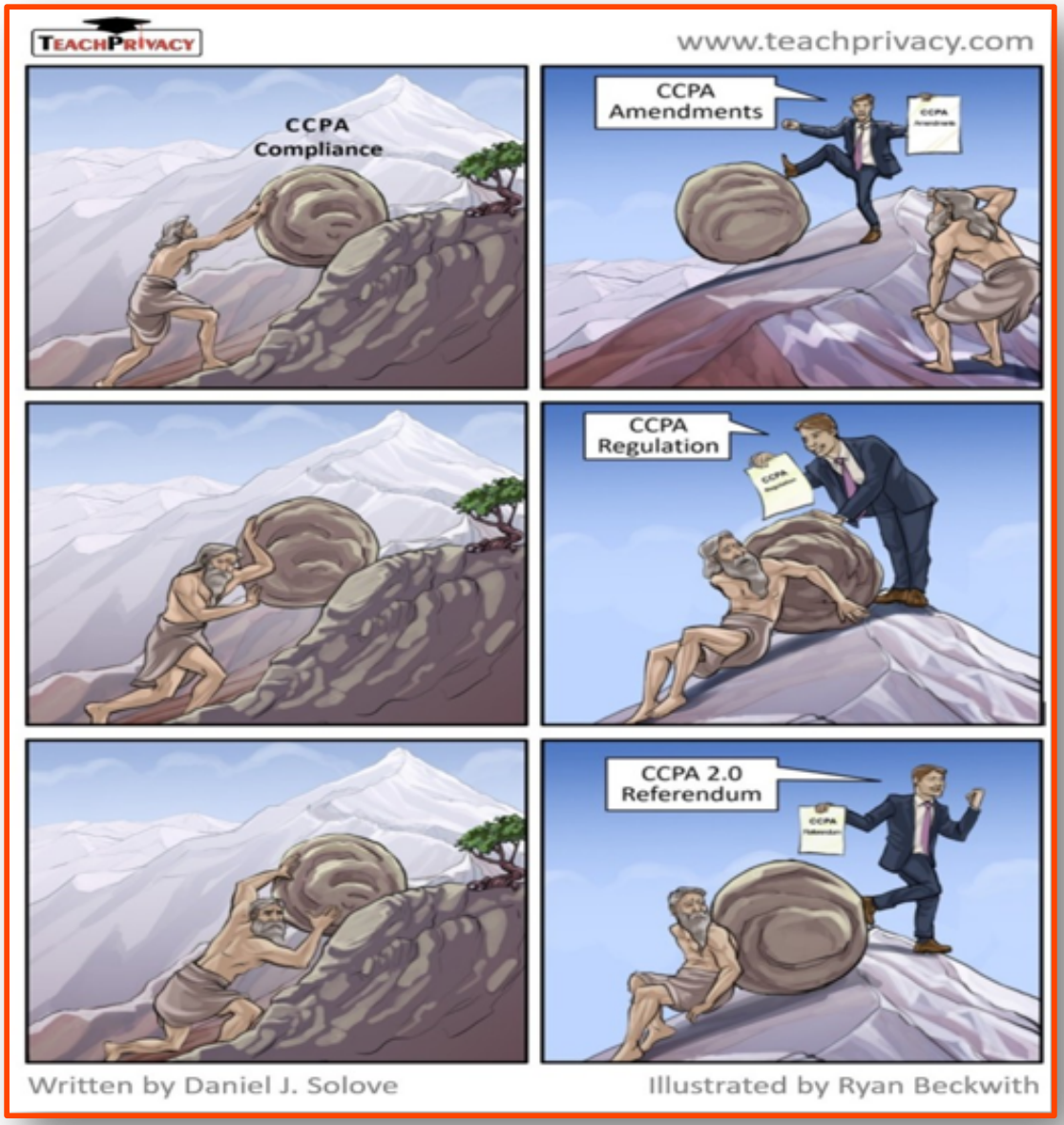


VA, NY, and WA Privacy Bill Comparison

	Virginia Senate Bill 1392	Washington Second Substitute Senate Bill 5062	New York Assembly Bill 680
Scope of Application	• 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% of gross revenue from the sale of personal data.	• Conducting business in Washington or • Produce products or services for Washington residents and • Process 100,000 consumers' data or process 25,000 consumers' data but derive over 25% of gross revenue from the sale of personal data.	• Applies to entities in New York State or those that produce products or services targeted intentionally to residents of New York State.
Effective Date	January 1, 2023	July 31, 2022	180 days after bill becomes law
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	30 days from receipt of request. Extendable once for an additional period of 60 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 issuance of a warning	✗
Private right of action	✗	✗	✓
Attorney General enforcement maximum penalty	$7,500 per violation	$7,500 per violation	Not specified. Each individual whose information was unlawfully processed counts as a separate violation and each provision that is violated counts as a separate violation.

California Consumer Privacy Act (CCPA)

The Impactful Uncertainty of CA Privacy Laws



CCPA Private Right of Action

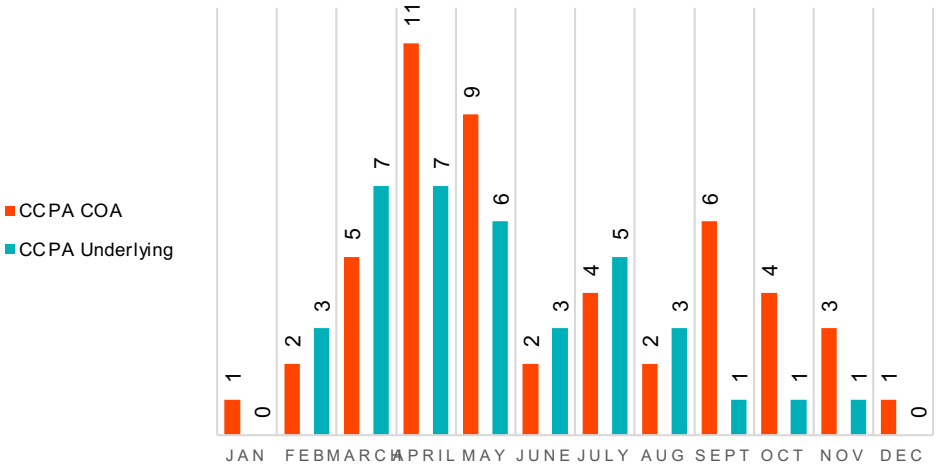
"(a) (1) Any consumer whose **nonencrypted and nonredacted personal information**, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an **unauthorized access and exfiltration, theft, or disclosure** *as a result of the business's violation of the duty to* ***implement and maintain reasonable security*** *procedures and practices appropriate to the nature of the information to protect the personal information* may institute a civil action for any of the following:

> (a) To recover damages in an amount not less than $100 and not greater than $750 per consumer per incident, whichever is **greater**;
>
> (b) Injunctive or declaratory relief;
>
> (c) Any other relief the court deems proper."

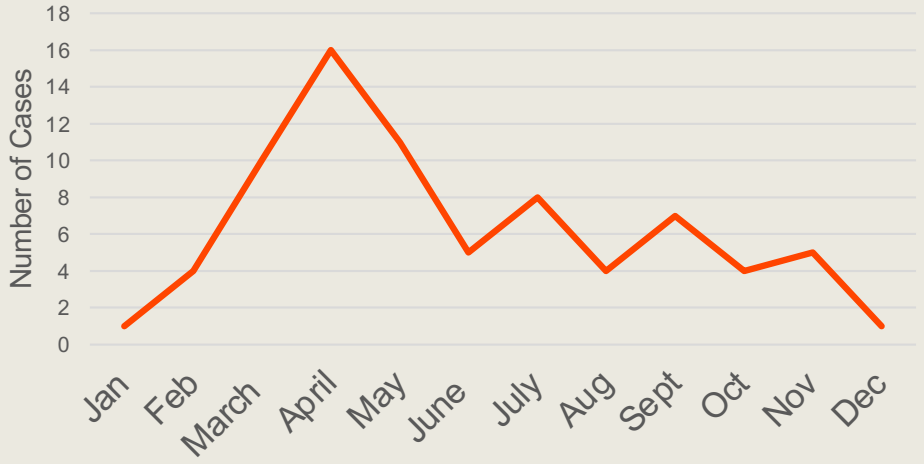
(Cal. Civ. Code § 1798.150(a)(1).)

CCPA Cases Filed in 2020

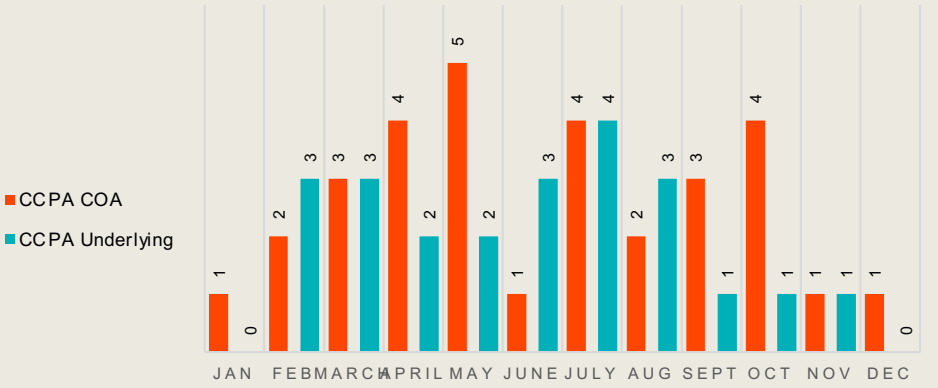
CCPA ALLEGATIONS IN 2020 BASED ON CASES FILED



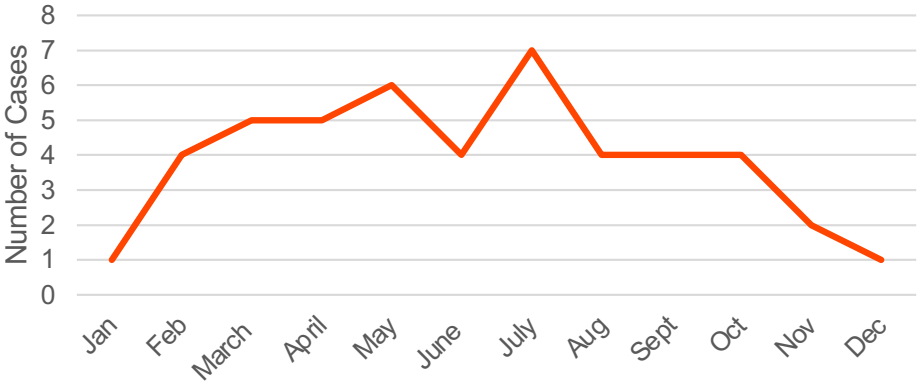
NUMBER OF CCPA CASES FILED EACH MONTH



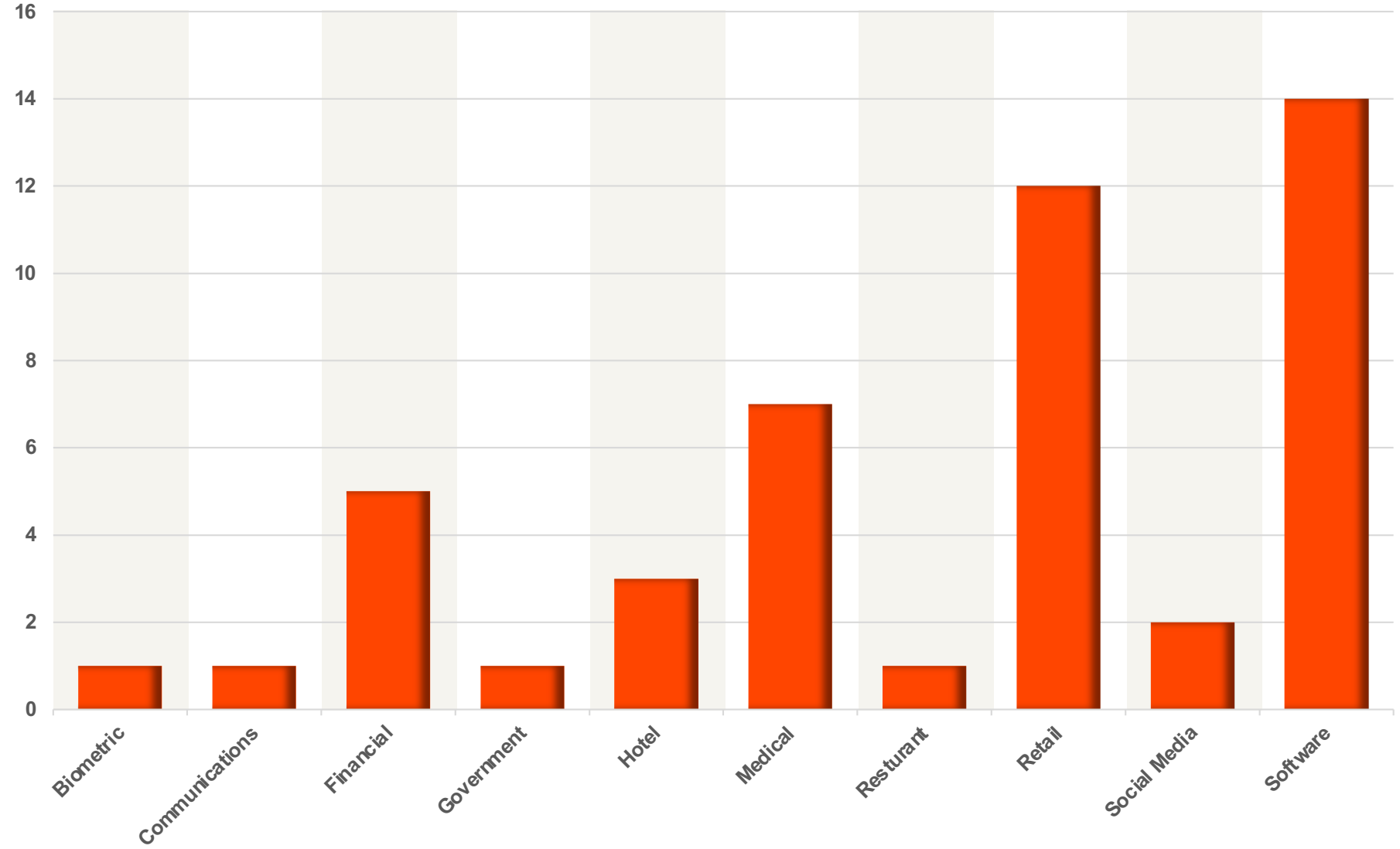
CCPA ALLEGATIONS IN 2020 BASED ON UNIQUE DEFENDANTS



NUMBER OF CCPA CASES FILED EACH MONTH UNIQUE DEFENDANTS



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



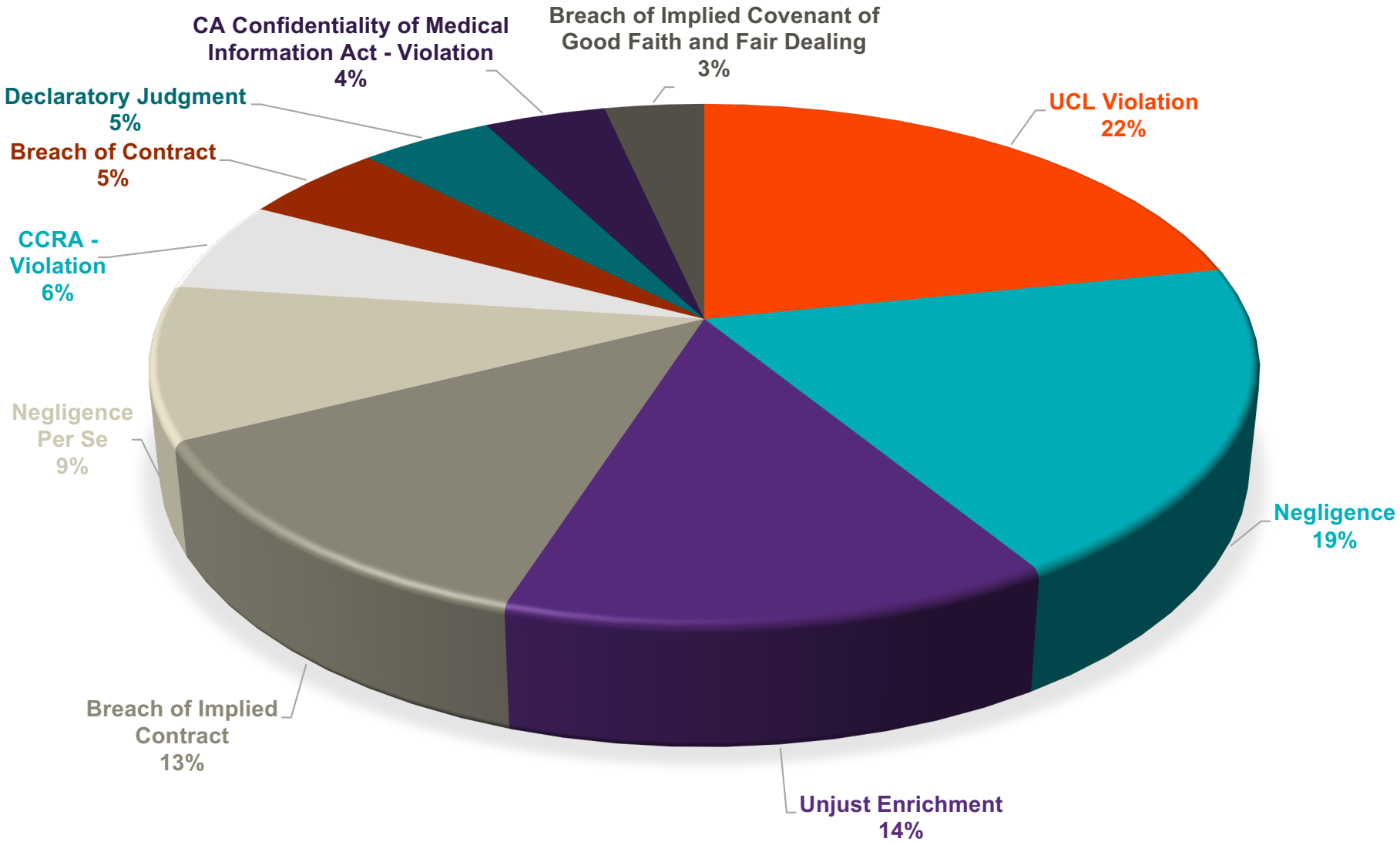
Where are CCPA Cases Being Filed?

- Since January 1, 2020, **61** cases have been filed in federal courts, and **15** cases in state court (through December 31, 2020).
- Unique defendants: **39** in federal court, **8** in state court.
- The majority of cases that cite to the CCPA have been filed in CA courts, but cases have also been filed in NY and FL.

Top Courts

Court	Cases	Unique Defendant Cases
Northern District of California	29	17
Central District of California	18	13
State Superior Court	15	8
Southern District of California	8	6

Other Common Causes of Action (%)



Takeaways

1. Federal court is plaintiffs' preferred venue for putative CCPA class actions.
2. More than half of all complaints alleging CCPA violations in 2020 did *not* allege that California residents' personal information was impacted due to a data breach.
3. Courts have not interpreted what it means to "do business" in California—thus which businesses must comply is an unsettled question.
4. CCPA claims have been paired with collateral claims brought under other California consumer protection statutes, most commonly the Unfair Competition Law.
5. The California Attorney General has not yet stepped into the arena by filing enforcement actions, though confidential notice letter have been issued to certain violators.
6. Non-California residents bringing CCPA claims will likely face Article III standing challenges in federal court.
7. Mandatory arbitration provisions and class action waivers are prohibited, ensuring consumers will bring their CCPA claims in public forums.
8. Though the CCPA provides a "safe harbor" provision by requiring consumers to provide 30 days' notice of violations and an opportunity to cure, in practice the safe harbor has not been frequently relied upon by defendants seeking dismissal of CCPA actions.

California Privacy Rights Act (CPRA)

CCPA Enforcement

Xavier Becerra, California Attorney General

"If they are not (operating properly) ... I will descend on them and make an example of them, to show that if you don't do it the right way, this is what is going to happen to you." –Xavier Becerra

Stacey Schesser, California Supervising Deputy Attorney General

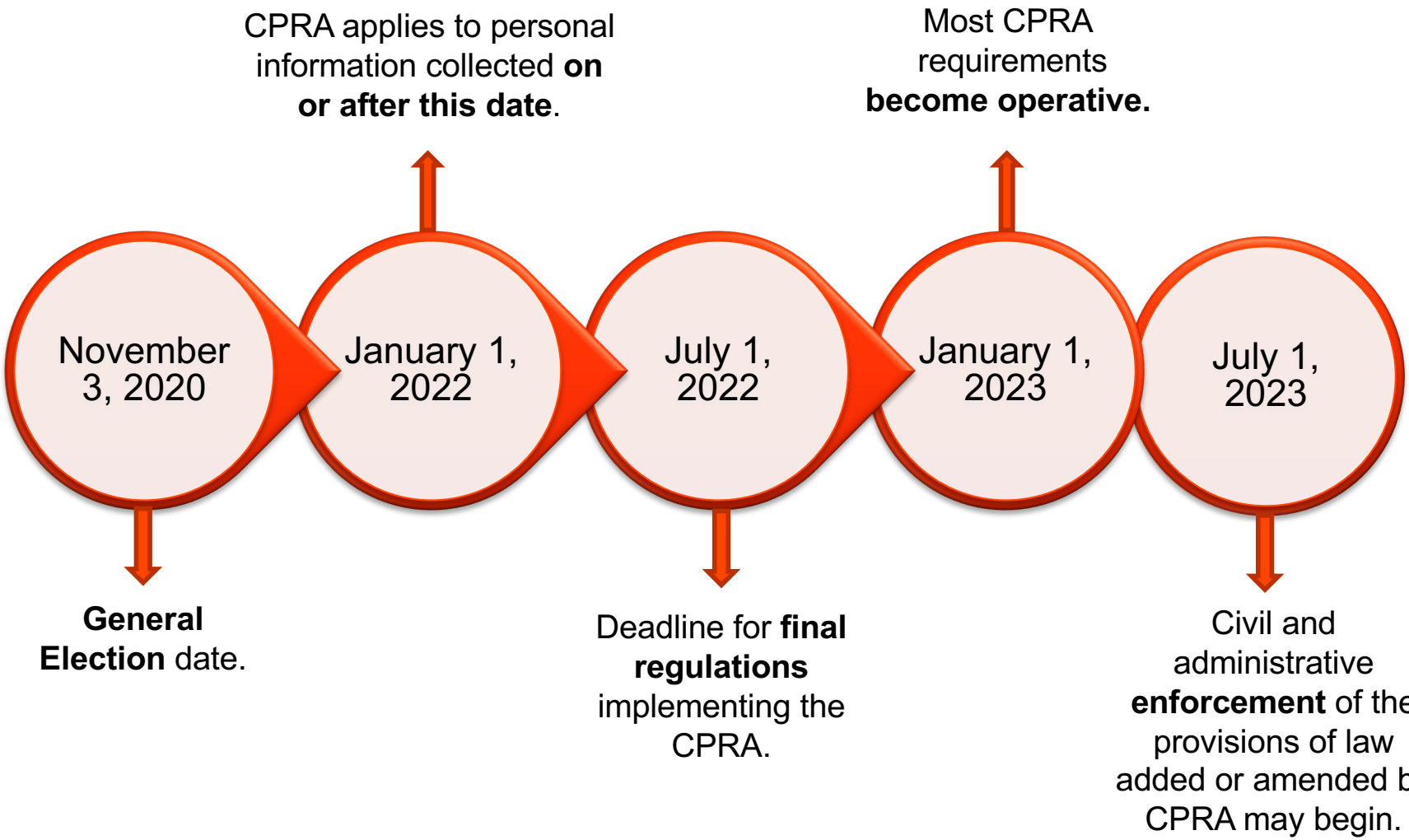
Gavin Newsom, California Governor

CPRA Changes the Privacy Landscape

- CPRA would make significant changes to the CCPA and would expand businesses' obligations.
- Creates a California Privacy Protection Agency (CPPA) and appoints a Chief Privacy Auditor.
  - Five member board.
  - Chair appointed by the Governor.
  - The Attorney General, Senate Rules Committee and Speaker of the Assembly shall each appoint a member of the board.
  - These appointments should be made from among Californians with expertise in the areas of privacy, technology, and consumer rights.

- On December 6, President-elect Biden selected former California Attorney General Xavier Becerra to Lead Health and Human Services.
  - Who will take over as Attorney General, and what are the implications for CPPA?
  - Governor of California will appoint the next CA Attorney General.

CPRA Key Dates



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	✗	✓

A Federal Fix?

What About a Federal Fix?

- Enacting a federal standard will continue to be a priority in 117th Congress.
- Main areas of disagreement—private right of action and state preemption—will remain.
- While enactment during this Congress is unlikely, additional hearings, discussions and efforts to find consensus will likely continue.

Senate Working Group

Federal Legislative Efforts: 116th Congress

Senate Commerce Republicans

- **Preemption**: Yes
- **PRA**: No
- **Authority**: FTC existing authority and state AGs.
- **Data Security**: FTC certification programs to create standards.
- **Rights**: access, correction, deletion, data portability

Senate Commerce Democrats

- **Preemption**: No
- **PRA**: Yes
- **Authority**: FTC new bureau and state AGs.
- **Data Security**: Corporate privacy officers, FTC/NIST rulemaking
- **Rights**: access, correction, deletion, data portability

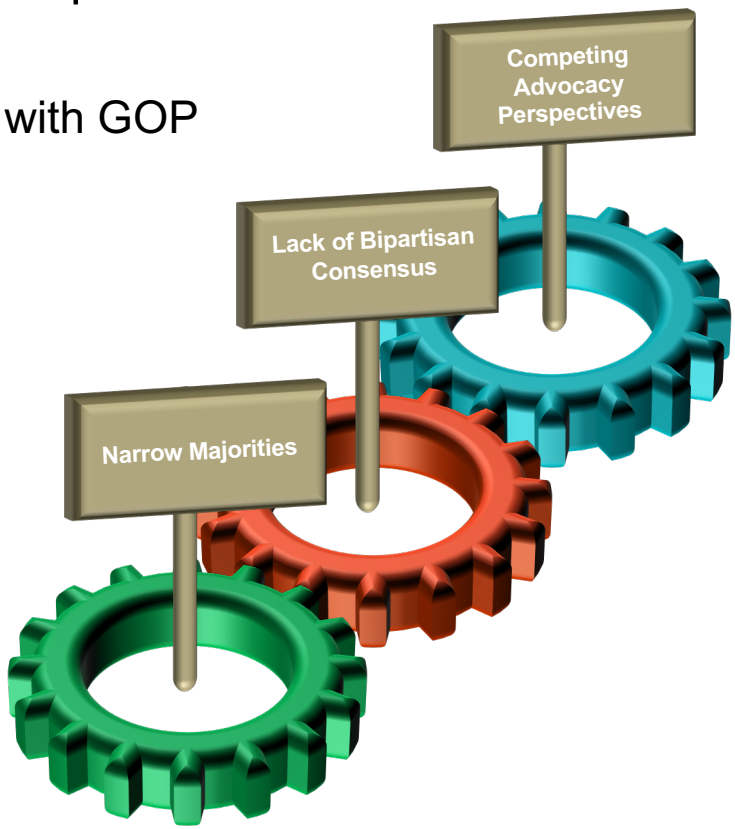
House Bipartisan Draft

- **Preemption**: No language
- **PRA**: No language
- **Authority**: FTC new privacy bureau.
- **Data Security**: Annual assessments, FTC rulemaking, breach notification
- **Rights**: access, correction, deletion, data portability

Significant Uncertainty Remains

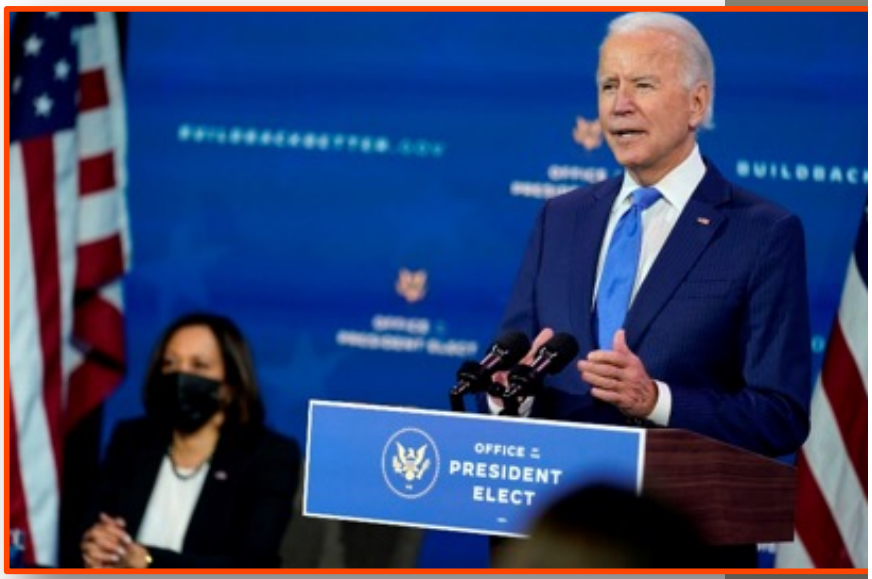
"We continue to be hopeful, but at this point, there isn't any path forward at the moment."
- Senate Majority Whip John Thune (R-SD) during the 116th Congress

- Narrow majorities in the Senate and House will require bipartisan support to advance any federal fix.
  - Unclear whether Democrats can reach agreement with GOP Members on privacy.
  - Committee hearings to continue.
  - Biden likely to support any bipartisan solution.
- Motivated advocacy pushing agenda.
  - Industry advocates vs. consumer activists.
  - State regulators pushing their own role.
  - Preemption and private right of action key issues.
- COVID-19.



What to Expect from the Biden Administration

- Hearings, hearings, hearings.
- Big Tech focus – antitrust, Section 230, data privacy.
- Artificial intelligence (AI).
- Continued state data privacy enforcement and regulation.
- Active state attorneys general in partnership with federal government.
- Republican Attorneys General Association (RAGA) & Democratic Attorneys General Association (DAGA).
- Cybersecurity supply chain and information sharing.
- Increased activity at the federal agency level.

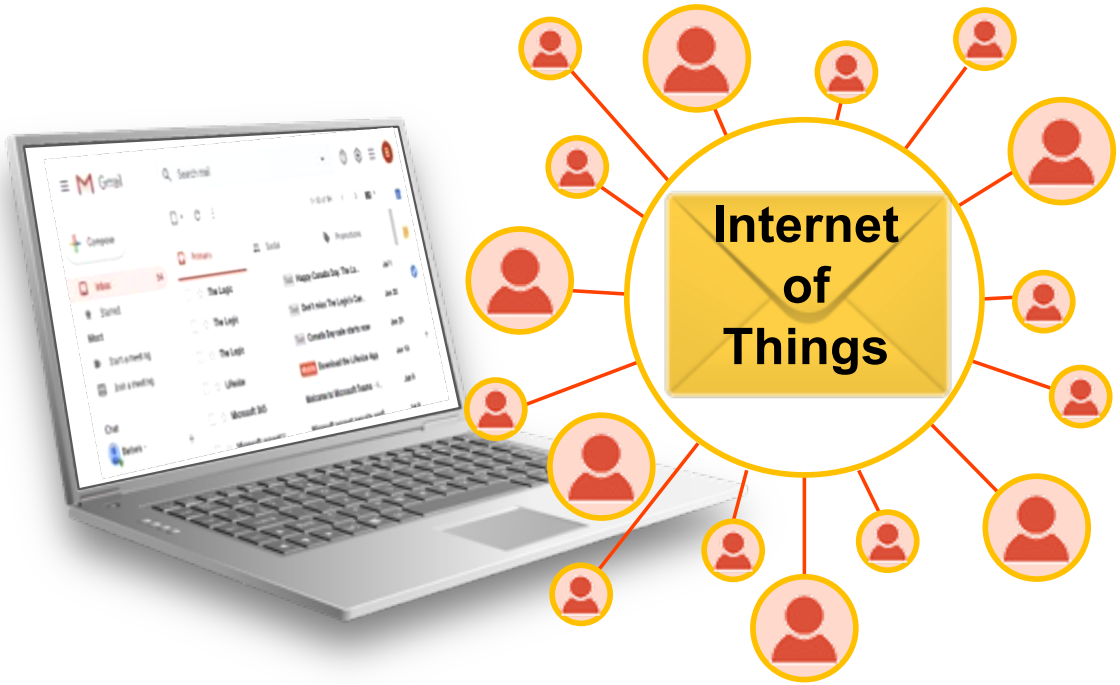


What to Expect from New Agency Heads

- Federal Trade Commission: Acting Chair Rebecca Kelly Slaughter.
  - Agency to take on a more aggressive role in policing tech giants.
  - Called for strong federal privacy legislation.
  - Focus on discriminatory algorithms and facial recognition.
- Consumer Financial Protection Bureau (CFPB): Rohit Chopra.
  - Former commissioner on the FTC who worked to increase the scrutiny of Big Tech corporations.
  - Expect a more aggressive and active CFPB on a number of fronts.

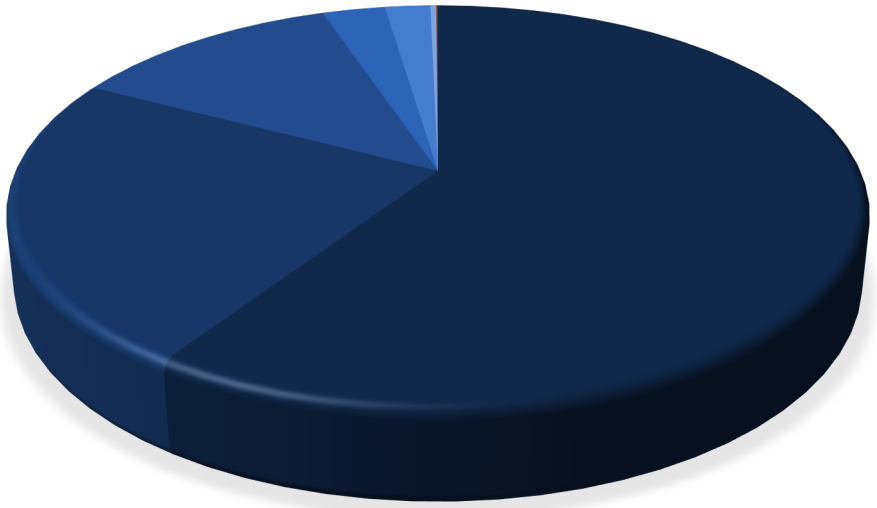
Developing Regulation of the Internet of Things

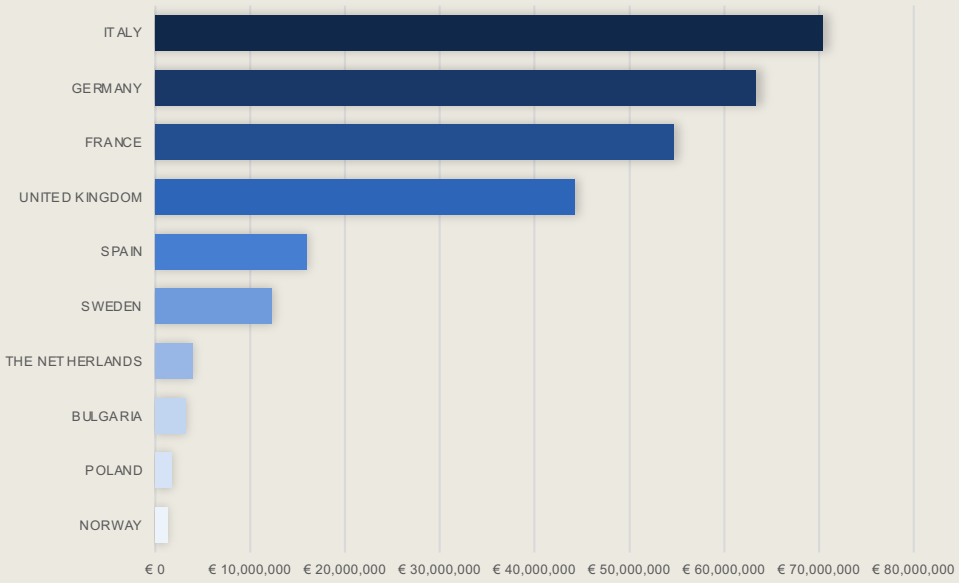
- On December 4, 2020, President Donald Trump signed H.R. 1668, the Internet of Things (IoT) Cybersecurity Improvement Act of 2020, into law.
- It would require NIST to develop standards and guidelines for the federal government on "the appropriate use and management by agencies of [IoT] devices owned or controlled by an agency and connected to information systems owned or controlled by an agency" within 180 days of enactment.



International Privacy Updates

Fines Under General Data Protection Regulation (GDPR) by Violation





	Violation	Sum of Fines
	Insufficient legal basis for data processing	€ 164,332,598 (at 120 fines)
	Insufficient technical and organizational measures to ensure information security	€ 64,546,532 (at 119 fines)
	Non-compliance with general data processing principles	€ 33,684,346 (at 89 fines)
	Insufficient fulfilment of data subjects rights	€ 7,791,725 (at 51 fines)
	Insufficient fulfilment of information obligations	€ 5,635,445 (at 30 fines)
	Insufficient fulfilment of data breach notification obligations	€ 733,291 (at 15 fines)
	Lack of appointment of data protection officer	€ 186,000 (at 5 fines)
	Insufficient cooperation with supervisory authority	€ 178,629 (at 24 fines)
	Insufficient data processing agreement	€ 14,380 (at 2 fines)
	Insufficient cooperation with supervisory authority	€ 4,400 (at 1 fines)
	Unknown	€ 500 (at 1 fines)
	Insufficient fulfilment of data breach obligations	€ 286 (at 1 fines)

	Country	Sum of Fines
	ITALY	**€ 70,393,601** (at 44 fines)
	GERMANY	**€ 63,386,633** (at 28 fines)
	FRANCE	**€ 54,661,300** (at 14 fines)
	UNITED KINGDOM	**€ 44,221,000** (at 4 fines)
	SPAIN	**€ 15,937,010** (at 185 fines)
	SWEDEN	**€ 12,332,430** (at 17 fines)
	THE NETHERLANDS	**€ 3,930,000** (at 7 fines)
	BULGARIA	**€ 3,210,690** (at 20 fines)
	POLAND	**€ 1,764,298** (at 20 fines)
	NORWAY	**€ 1,276,450** (at 19 fines)

Data from https://www.enforcementtracker.com/

Massive Fines Continue to be the New Normal?

H&M Germany fined $41.3M in one of largest GDPR penalties

By Jaclyn Jaeger | Thu, Oct 1, 2020 12:56 PM

- H&M Germany was fined $41.3M for GDPR violations related to excessive monitoring of several hundred employees.

INTERNATIONAL • DATA BREACH

A Huge Data Breach Fine Against British Airways Is a Warning to Global Execs

By Jeremy Kahn July 8, 2019

- On October 16, 2020, the ICO announced that it had fined British Airways approx. $27M for a data breach which compromised the personal data of more than 400,000 of the airlines' customers, an 89% reduction from the initial penalty proposed on July 4, 2019 (approx. $253M).

French Data Protection Body Fines Google and Amazon Over Cookie Policy

Regulators fined Google €100 million and Amazon €35 million for placing advertising cookies on users' computers without obtaining prior consent or providing adequate information.

By Anne Bagamery | December 11, 2020 at 12:26 PM | The original version of this story was published on Law.com International

- In December 2020, France's data protection agency, the CNIL, hit Google ($120M) and Amazon (~$42M) with fines for dropping tracking cookies without consent.

EU-U.S. Privacy Shield

Schrems II – Timeline

*C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems ("**Schrems II**")*

- **July 16, 2020** – The Court of Justice of the European Union (CJEU) in the Schrems II decision struck down the EU-U.S. Privacy Shield with immediate effect.
- CJEU held that Standard Contractual Clauses (SCCs), another mechanism to transfer data outside the EU and the U.K., can still in principle be relied upon, **but** supplementary measures may be necessary in case of transfers to certain jurisdictions.
- **November 10, 2020** – The European Data Protection Board (EDPB) published draft Guidance on Supplementary Measures and recommendations on Surveillance Measures.
- **November 12, 2020** – The European Commission published new, updated and modernised draft SCCs for the transfer of personal data outside the EEA (New SCCs), and a separate draft set of Article 28 SCCs between controllers and processors (for EU companies).
- **January 15, 2021** – The EDPB and European Data Protection Supervisor adopted joint opinions on both sets of draft SCCs, endorsing them and providing comments.
- New SCCs and final Guidance on Supplementary Measures expected to be formally adopted in Q1/Q2 2021.

Schrems II – Key Takeaways

- Businesses relying exclusively on the Privacy Shield for transfers of data from the EU and the UK to the U.S. should discontinue such reliance as soon as feasible.
- Consider what alternative mechanisms other than the Privacy Shield for international personal data transfers could be relied on.
- Prioritize dealings: The regulators in certain EU Member States have more appetite for investigation, and have made bold statements (see Berlin authority: “Now is the hour for Europe's digital independence.”); other regulators like the UK said their approach would be pragmatic.
- Limit data to be transferred outside the EU/UK, wherever possible.
- Prioritize dealing with high risk transfers.
- Consider adopting global information sharing agreement and data transfer agreement.
- Internally record how your company processes requests from government and law enforcement.
- Political solution: Privacy Shield take 3?
  - In October 2020, the U.S. Department of Commerce and the European Commission announced they had initiated discussions to evaluate the potential for an enhanced EU-U.S. Privacy Shield framework to comply with the Schrems II decision.

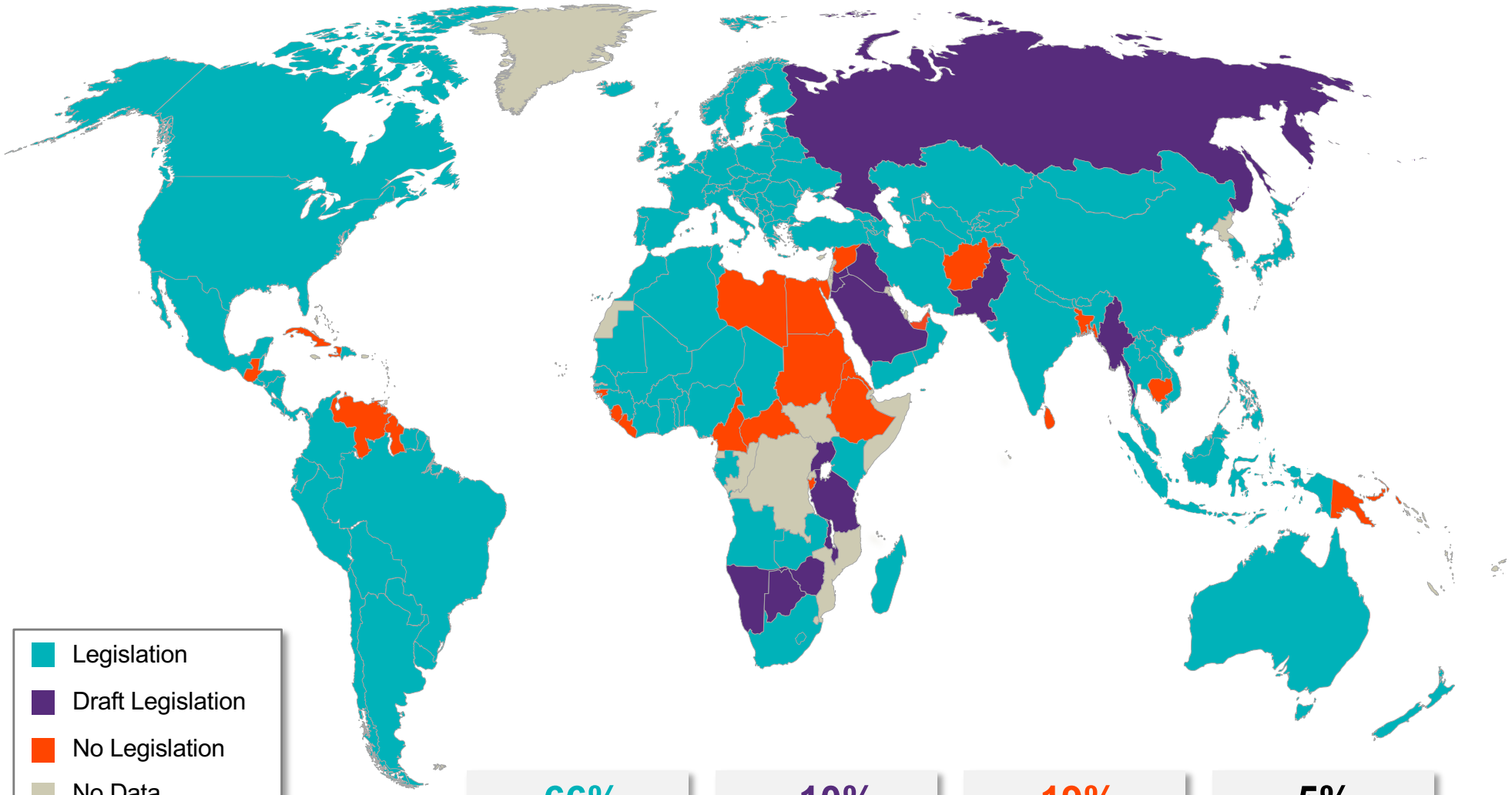
Schrems II – Enforcement Timeline

- **July 16, 2020** – EU-U.S. Privacy Shield is struck down with immediate effect, causing chaos and confusion.
- **July 17, 2020** – Berlin DPA takes hardline position, suggesting companies should move their data from the U.S. to the EU, and that SCCs cannot continue.
- **Late July 2020** – Finland DPA begins Schrems II probes, contacting companies such as Amazon Web Services, Microsoft and IBM – to get information about their response to the landmark decision.
- **August 18, 2020** – Schrems' activist group noyb filed 101 identical complaints to DPAs across Europe, in an attempt to force regulators to enforce the landmark Schrems II ruling.
- **September 4, 2020** – European DPA launches taskforce to investigate Schrems II's 101 complaints.
- **September 8, 2020** – Swiss Privacy Shield deemed inadequate by Switzerland's DPA.
- **September 14, 2020** – Irish Data Protection Commission launches investigation into Facebook's use of SCCs.
- **September 28, 2020** – 33 prominent companies have revealed how legal departments are responding to the Schrems II judgment – with many organizations leaning heavily on SCCs.
- **October 14, 2020** – A French administrative judge refused to order France's health database to stop processing personal information on Microsoft's cloud, despite Schrems II-driven fears that U.S. intelligence could access it.
- **October 29, 2020** – The European Data Protection Supervisor warned the EU institutions it regulates not to set up any new transfers to the US.
- **February 19, 2021** – German DPAs set up a taskforce to start contacting companies as early as next week about their response to the Schrems II judgment.

Brexit

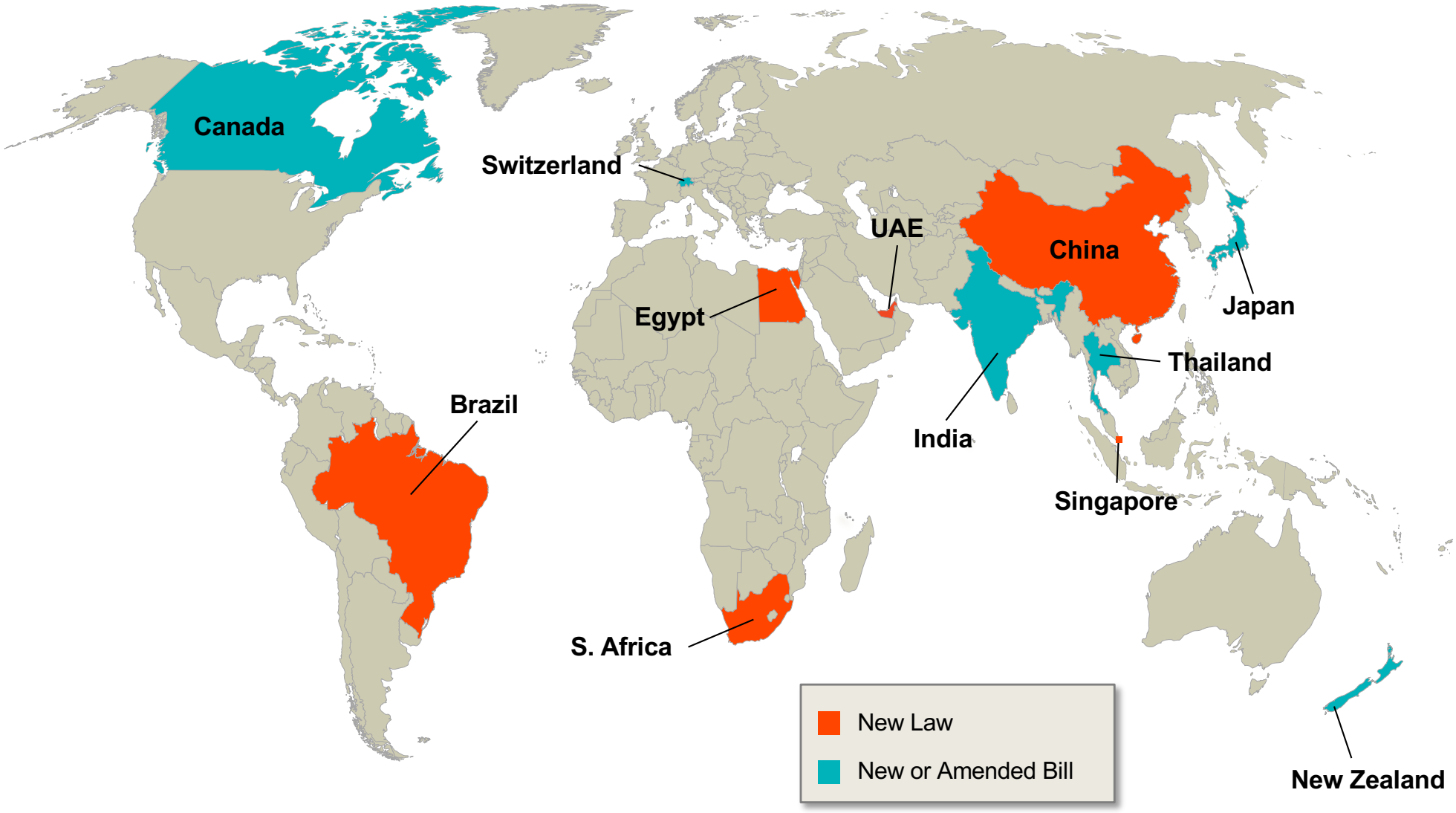
- The U.K. left the EU on January 31, 2020. A transition period ended on December 31, 2020, during which matters proceeded as if the U.K. continued to be part of the EU.
- On December 24, 2020, the EU and the U.K. adopted a Trade and Cooperation Agreement, touching on personal data matters.
- U.K.-EU personal data flows
  - U.K. declared that, on a temporary basis, it deemed "adequate" the EEA countries and the other countries approved by the European Commission. Data flows from the UK to those countries can continue freely.
  - Temporary measure allowing the EU to transfer to the U.K. until end of Q2 2021.
  - Some uncertainty if the EU will declare the U.K. a jurisdiction offering "adequate" protection. Positive noises: on February 15, 2021, it was reported that a draft adequacy decision for the U.K. had been prepared by the European Commission.
- **The U.K. GDPR:** The EU GDPR, in the form it was pre-Brexit, has been retained as part of U.K. domestic law, and is now called the "U.K. GDPR". The U.K. GDPR, which is materially the same as the EU GDPR, sits alongside the U.K. Data Protection Act 2018, as amended.
- **EU/U.K. Representatives:** Any businesses that are based outside the EEA or outside the U.K., but are nevertheless within the scope of the EU/U.K. GDPR, have to consider whether to appoint a so-called EU/U.K. representative.

Regulators Around the World



66%	10%	19%	5%
COUNTRIES WITH **LEGISLATION**	COUNTRIES WITH **DRAFT LEGISLATION**	COUNTRIES WITH **NO LEGISLATION**	COUNTRIES WITH **NO DATA**

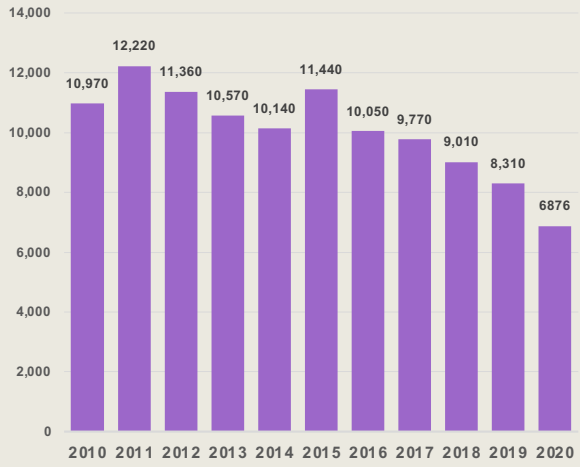
Major Legislative Developments Around the World in 2020

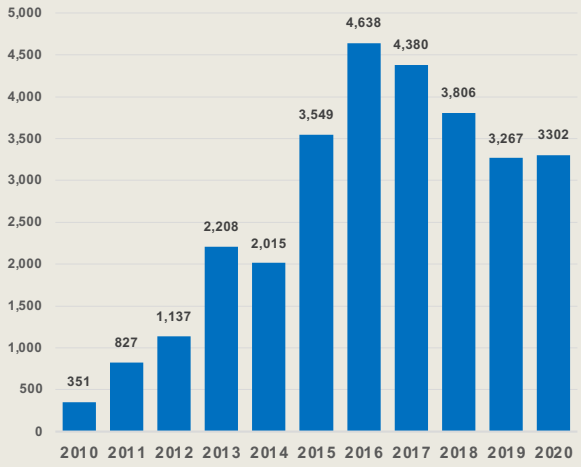


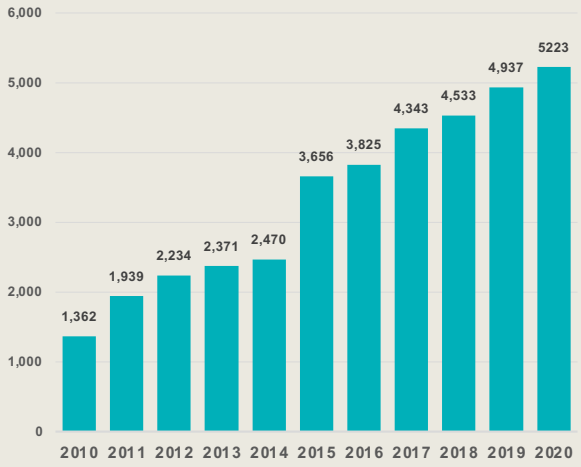
Privacy & Data Breach Class Action Updates

Privacy Class Action Trends

- FCRA lawsuits continue to steadily increase from 2010-2020.
- Total TCPA cases have declined, but the percent of consumer class actions continue to climb.
- FDCPA cases declined 17.6% from 2019 to 2020.







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.
- Potential for federal legislation could lead to wave of biometric litigation.
  - National Biometric Information Privacy Act of 2020 (Sanders/Merkley)

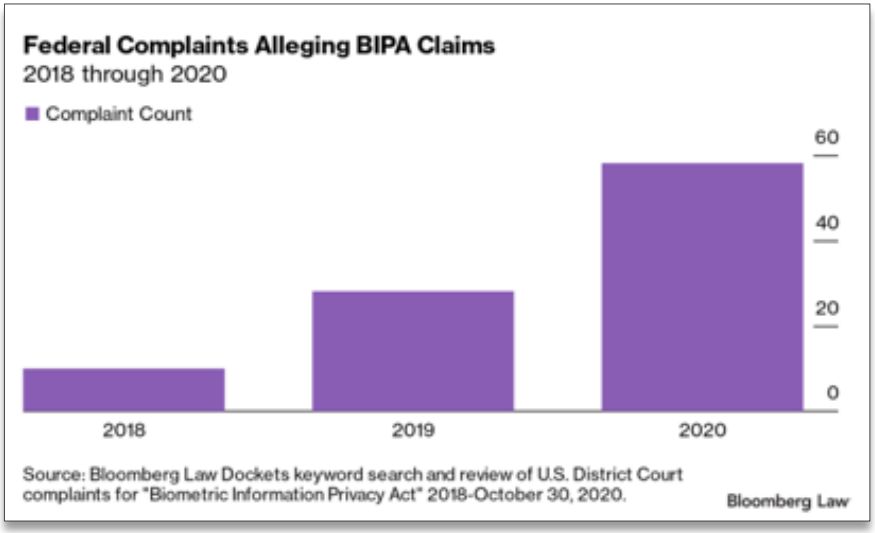
LAW360

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.



Data Breach Trends

- The number of data breaches in 2020 was more than **double** that of 2019.
- 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.
- 2020 also demonstrated that legal fallout from breaches can extend to company executives (Uber).
- Capital One case – Forensic reports no longer privileged?

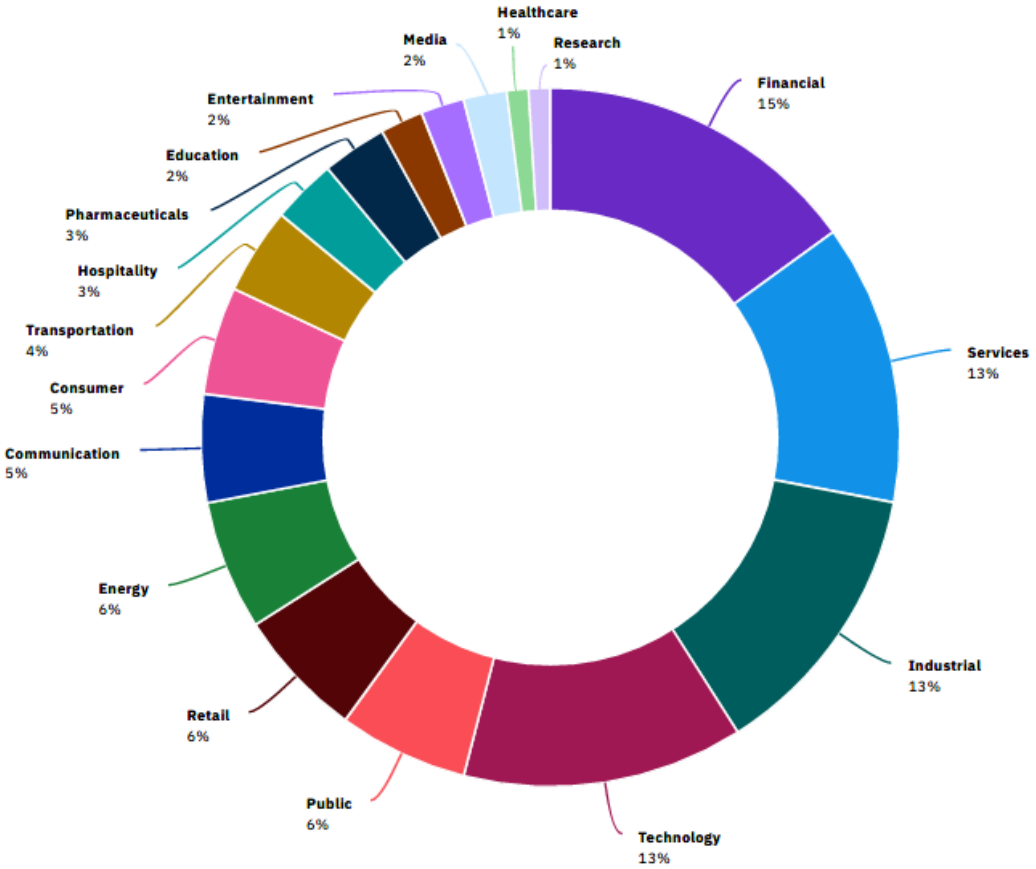


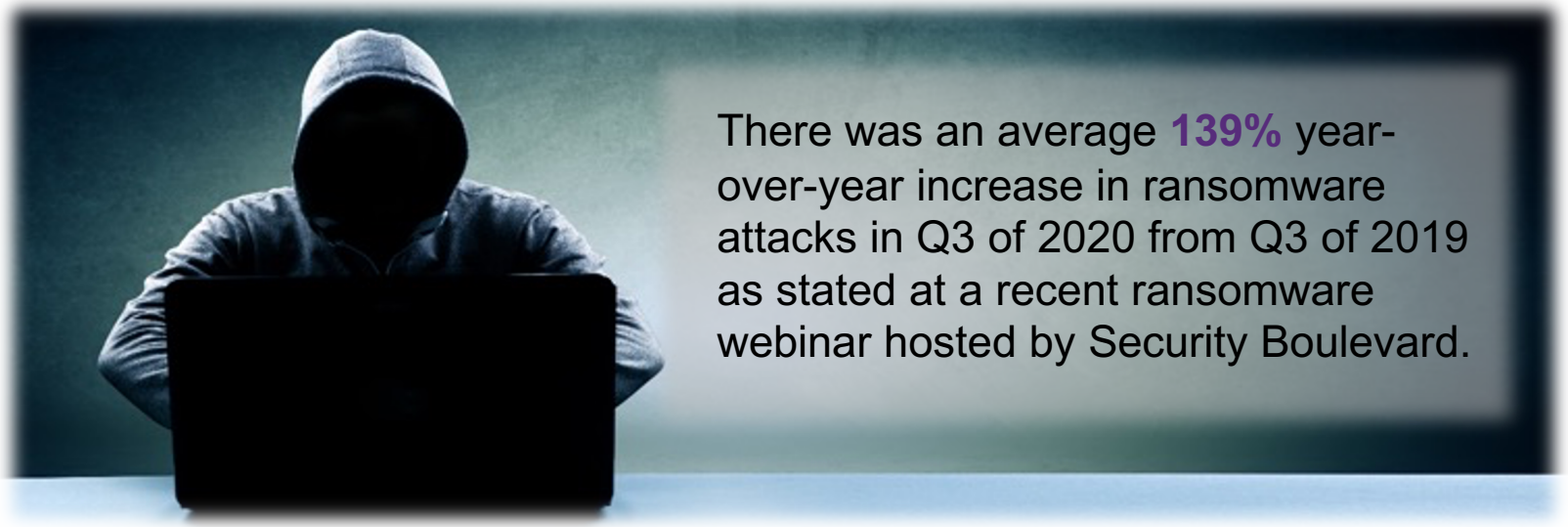
Chart from IBM Security Cost of a Data Breach Report 2020

Protecting Privilege: Top 10 Checklist for Cybersecurity Forensic Investigation Reports

- ☑ Retain outside counsel to manage the investigation.
- ☑ Add—don't replace—a cybersecurity vendor to provide services necessary for the rendering of legal advice.
- ☑ Avoid using stock language in the statement of work.
- ☑ Think critically about requesting a written report of findings.
- ☑ Create segmented teams to protect the privilege.
- ☑ Limit distribution of privileged attorney work product.
- ☑ Keep track of where the written findings are shared and why.
- ☑ Prepare a separate, non-privileged incident report that can be shared.
- ☑ Pay expenses from the legal budget.
- ☑ Be prepared for disclosure.

Supply Chain Cyber Incidents in 2020

Ransomware



Ransomware attacks have caught the attention of regulators, with recent advisories including:

- On February 4, 2021, the New York Department of Financial Services (NYDFS) issued Circular Letter No. 2, "Cyber Insurance Risk Framework" where they note being particularly concerned with ransomware attacks.
- In October 2020, the United States Department of Treasury's Office of Foreign Assets Control (OFAC) issued an advisory, warning of the potential risk of sanctions to companies and individuals who make ransomware payments.
- In July 2020, the Office of Compliance Inspections and Examinations (OCIE) released a Risk Alert regarding the increasing frequency and sophistication of ransomware attacks targeting U.S. Securities and Exchange Commission (SEC) registrants.

Regulatory Enforcement

Regulatory Data Privacy Settlements

Zoom Video Communications, Inc.

- The FTC reached a nonmonetary settlement with Zoom, over misleading consumers on the company's cybersecurity practices regarding end-to-end encryption. The settlement required Zoom to implement a comprehensive information security program.

Everalbum, Inc.

- In another nonmonetary settlement, the FTC reached an agreement on allegations that Everalbum deceived its customers about the use of facial recognition technology, and the retention of photos and videos of users who had deactivated their accounts. The settlement required Everalbum to delete the facial recognition data, as well as the recognition models and algorithms used to collect the data.

Google LLC and YouTube, LLC

- The FTC and Google reached $170 million settlement over allegations that YouTube illegally collected personal information from children, without their parents' consent.

Privacy Shield Enforcement

- FTC brought actions against a number of companies alleged to have made false claims of certification under the EU-U.S. Privacy Shield and continues to express that enforcement in this area is a high priority.

Ongoing Investigations in 2021

DOJ – Apple, Amazon, Google, Others?

- The Trump Administration's DOJ focused its investigating power on whether "market-leading online platforms…are engaging in practices that have reduced competition, stifled innovation, or otherwise harmed consumers."

FTC – Social Media, Health Apps, Facial Recognition

- The FTC is investigating reports that TikTok has violated a 2019 consent decree concerning children's privacy, as well Twitter, for misusing individuals personal information (PI) by disclosing the PI to advertisers.
- The FTC has indicated that the new administration will focus on health apps, including telehealth and contract tracing apps, where usage has exploded during the COVID-19 pandemic. The FTC is also focusing on facial recognition technology, and plans to actively investigation biased algorithms.

State AGs – Sabre Corp., Maple Media, LLC

- State AG's are investigating Sabre Corp. regarding data breaches that resulted in the PI of millions of consumers being stolen.
- State AG's have brought a case against Maple Media LLC and its subsidiary Super Basic LLC for collecting children's PI, and allowing third-party advertisers to collect data from children, without parental consent.

Takeaways

Top Privacy Concerns for Management

Increased Civil Litigation Risk

Insufficient Compliance

Evolving Regulatory International, National and State Privacy Landscape

Heightened Regulatory Focus on Regulatory Scrutiny in the Covid Era

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

Privacy Shield and Brexit Impact on GDPR

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.

CPRA – Impact of CRPA to strengthen CCPA and EU negotiations.

Federal Rulemaking – HIPAA, Gramm-Leach-Bliley, COPPA.

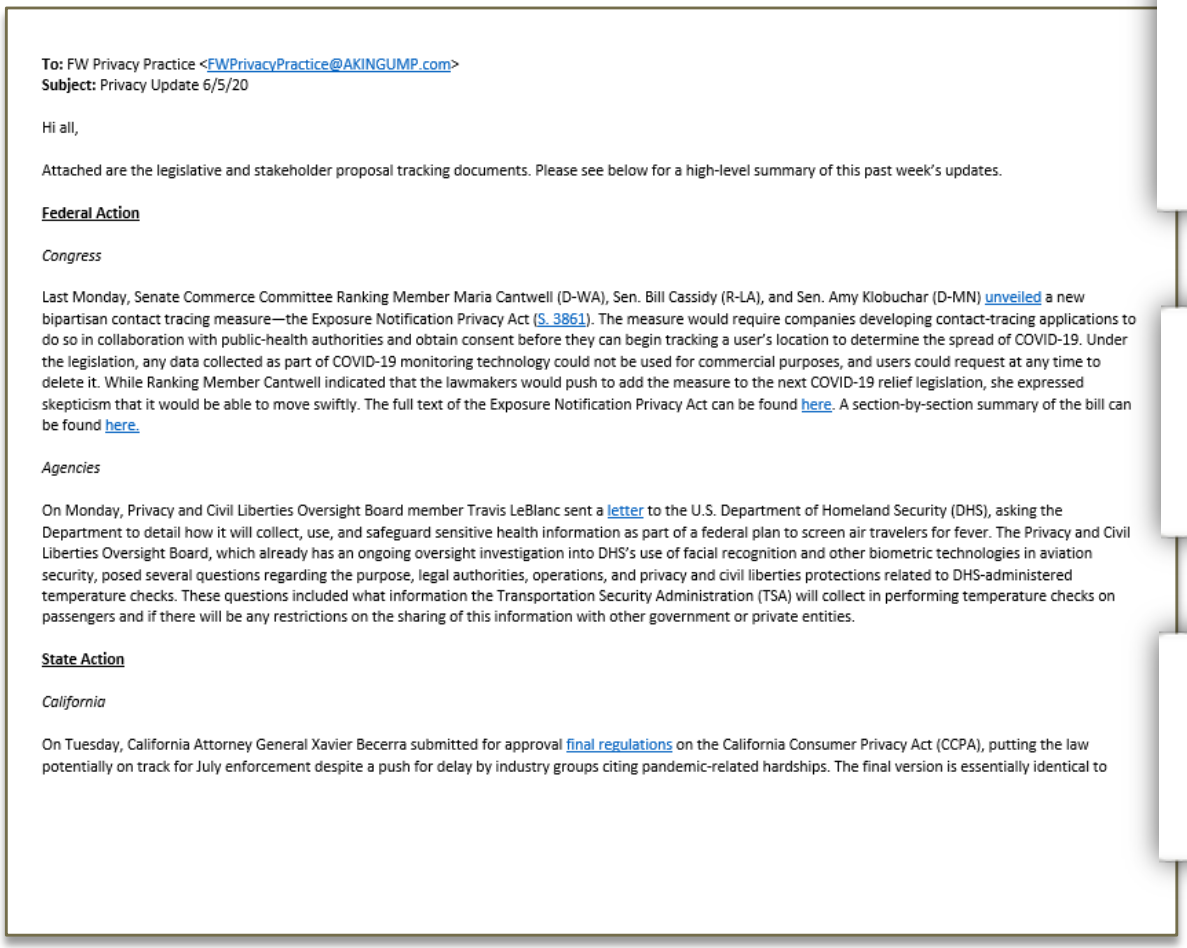
Facial Recognition/Biometrics – Expanding legislation and expensive litigation.

Future of Cross-Border Data Transfers

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

Akin Gump Privacy Policy Updates

- **Weekly federal privacy policy update emails.**



To: FW Privacy Practice <FWPrivacyPractice@AKINGUMP.com>
Subject: Privacy Update 6/5/20

Hi all,

Attached are the legislative and stakeholder proposal tracking documents. Please see below for a high-level summary of this past week's updates.

Federal Action

Congress

Last Monday, Senate Commerce Committee Ranking Member Maria Cantwell (D-WA), Sen. Bill Cassidy (R-LA), and Sen. Amy Klobuchar (D-MN) unveiled a new bipartisan contact tracing measure—the Exposure Notification Privacy Act (S. 3861). The measure would require companies developing contact-tracing applications to do so in collaboration with public-health authorities and obtain consent before they can begin tracking a user's location to determine the spread of COVID-19. Under the legislation, any data collected as part of COVID-19 monitoring technology could not be used for commercial purposes, and users could request at any time to delete it. While Ranking Member Cantwell indicated that the lawmakers would push to add the measure to the next COVID-19 relief legislation, she expressed skepticism that it would be able to move swiftly. The full text of the Exposure Notification Privacy Act can be found here. A section-by-section summary of the bill can be found here.

Agencies

On Monday, Privacy and Civil Liberties Oversight Board member Travis LeBlanc sent a letter to the U.S. Department of Homeland Security (DHS), asking the Department to detail how it will collect, use, and safeguard sensitive health information as part of a federal plan to screen air travelers for fever. The Privacy and Civil Liberties Oversight Board, which already has an ongoing oversight investigation into DHS's use of facial recognition and other biometric technologies in aviation security, posed several questions regarding the purpose, legal authorities, operations, and privacy and civil liberties protections related to DHS-administered temperature checks. These questions included what information the Transportation Security Administration (TSA) will collect in performing temperature checks on passengers and if there will be any restrictions on the sharing of this information with other government or private entities.

State Action

California

On Tuesday, California Attorney General Xavier Becerra submitted for approval final regulations on the California Consumer Privacy Act (CCPA), putting the law potentially on track for July enforcement despite a push for delay by industry groups citing pandemic-related hardships. The final version is essentially identical to

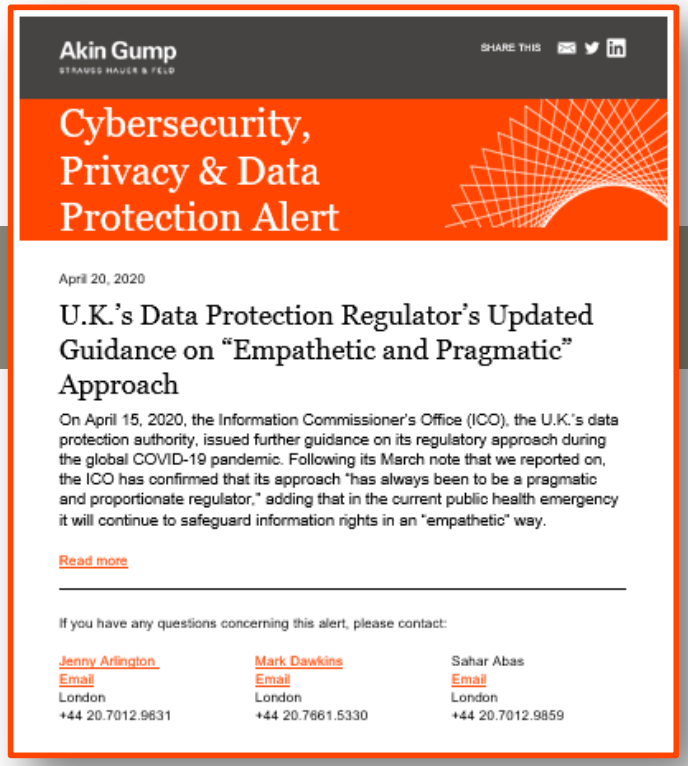
"Love the new format. Much easier to digest. Looks great and is as useful as always."

"This is the only privacy newsletter out of the far too many I am subscribed to that I actually read.☺"

"I continue to find these updates extremely valuable so thanks for sharing."

Akin Gump Resources

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


Akin Gump
STRAUSS HAUER & FELD

SHARE THIS

Cybersecurity, Privacy & Data Protection Alert

April 20, 2020

U.K.'s Data Protection Regulator's Updated Guidance on "Empathetic and Pragmatic" Approach

On April 15, 2020, the Information Commissioner's Office (ICO), the U.K.'s data protection authority, issued further guidance on its regulatory approach during the global COVID-19 pandemic. Following its March note that we reported on, the ICO has confirmed that its approach "has always been to be a pragmatic and proportionate regulator," adding that in the current public health emergency it will continue to safeguard information rights in an "empathetic" way.

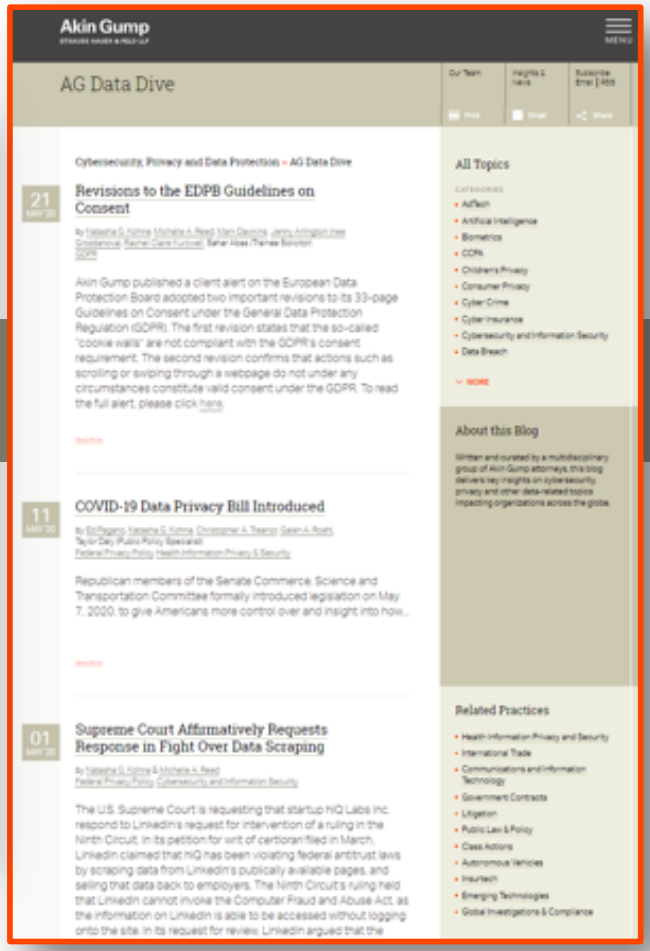
Read more

If you have any questions concerning this alert, please contact:

Jenny Arlington
Email
London
+44 20.7012.9631

Mark Dawkins
Email
London
+44 20.7661.5330

Sahar Abas
Email
London
+44 20.7012.9859


Akin Gump

AG Data Dive

Cybersecurity, Privacy and Data Protection > AG Data Dive

21 MAY 20

Revisions to the EDPB Guidelines on Consent

Akin Gump published a client alert on the European Data Protection Board adopted two important revisions to its 33-page Guidelines on Consent under the General Data Protection Regulation (GDPR). The first revision states that the so-called "cookie walls" are not compliant with the GDPR's consent requirement. The second revision confirms that actions such as scrolling or swiping through a webpage do not under any circumstances constitute valid consent under the GDPR. To read the full alert, please click here.

11 MAY 20

COVID-19 Data Privacy Bill Introduced

Republican members of the Senate Commerce, Science and Transportation Committee formally introduced legislation on May 7, 2020, to give Americans more control over and insight into how...

01 MAY 20

Supreme Court Affirmatively Requests Response in Fight Over Data Scraping

The U.S. Supreme Court is requesting that startup hiQ Labs Inc. respond to LinkedIn's request for intervention of a ruling in the Ninth Circuit. In its petition for writ of certiorari filed in March, LinkedIn claimed that hiQ has been violating federal antitrust laws by scraping data from LinkedIn's publically available pages, and selling that data back to employers. The Ninth Circuit's ruling held that LinkedIn cannot invoke the Computer Fraud and Abuse Act, as the information on LinkedIn is able to be accessed without logging onto the site. In its request for review, LinkedIn argued that the

All Topics

- AdTech
- Artificial Intelligence
- Biometrics
- CCPA
- Children's Privacy
- Consumer Privacy
- Cyber Crime
- Cyber Insurance
- Cybersecurity and Information Security
- Data Breach

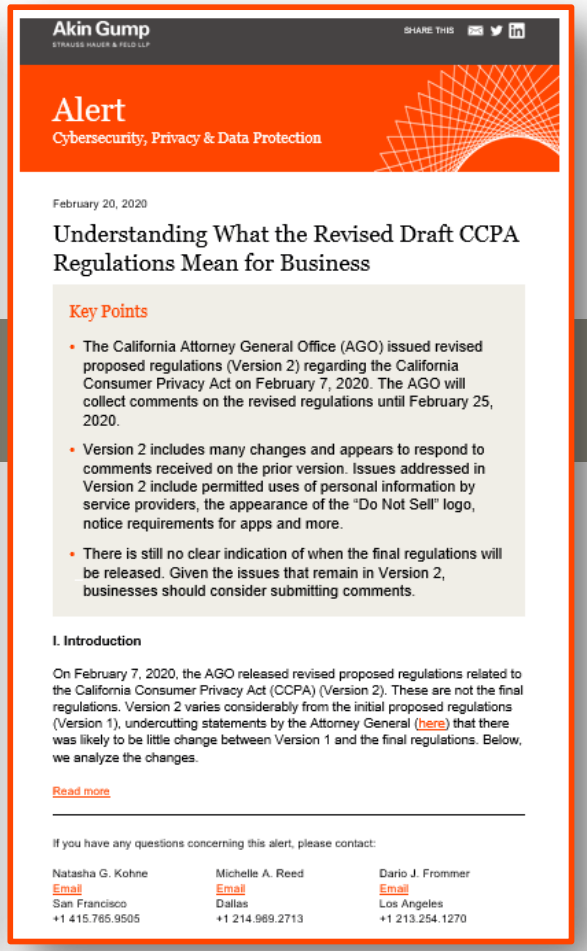
MORE

About this Blog

Written and curated by a multidisciplinary group of Akin Gump attorneys, this blog delivers key insights on cybersecurity, privacy and other data-related topics impacting organizations across the globe.

Related Practices

- Health Information Privacy and Security
- International Trade
- Communications and Information Technology
- Government Contracts
- Litigation
- Public Law & Policy
- Class Actions
- Autonomous Vehicles
- Insurtech
- Emerging Technologies
- Global Investigations & Compliance


Akin Gump
STRAUSS HAUER & FELD LLP

SHARE THIS

Alert
Cybersecurity, Privacy & Data Protection

February 20, 2020

Understanding What the Revised Draft CCPA Regulations Mean for Business

Key Points

- The California Attorney General Office (AGO) issued revised proposed regulations (Version 2) regarding the California Consumer Privacy Act on February 7, 2020. The AGO will collect comments on the revised regulations until February 25, 2020.
- Version 2 includes many changes and appears to respond to comments received on the prior version. Issues addressed in Version 2 include permitted uses of personal information by service providers, the appearance of the "Do Not Sell" logo, notice requirements for apps and more.
- There is still no clear indication of when the final regulations will be released. Given the issues that remain in Version 2, businesses should consider submitting comments.

I. Introduction

On February 7, 2020, the AGO released revised proposed regulations related to the California Consumer Privacy Act (CCPA) (Version 2). These are not the final regulations. Version 2 varies considerably from the initial proposed regulations (Version 1), undercutting statements by the Attorney General (here) that there was likely to be little change between Version 1 and the final regulations. Below, we analyze the changes.

Read more

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Email
San Francisco
+1 415.765.9505

Michelle A. Reed
Email
Dallas
+1 214.969.2713

Dario J. Frommer
Email
Los Angeles
+1 213.254.1270

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

Amy Purcell
Chief Privacy Officer, Senior Counsel, Vanguard
Wayne, PA
T: 610.669.9548
amy_purcell@vanguard.com

Anthony T. Pierce
Partner, Akin Gump Strauss Hauer & Feld LLP
Washington, D.C.
T: 202.887.4411
apierce@akingump.com

Appendix –Cited Material

- Virginia Consumer Data Protection Act, H.B. 2307/S.B. 1392 (Va. 2021)
- NYDFS Cybersecurity Regulation, 23 NYCRR 500 (N.Y. 2017)
- Stop Hacks and Improve Electronic Data Security (SHIELD Act) (N.Y. 2019)
- S.B. S567, 2021-2022 Leg. Sess. (N.Y. 2021)
- New York Privacy Act, A.B. A680, 2021-2022 Leg. Sess. (N.Y. 2021)
- Washington Privacy Act; S.B. 5062, 2021-2022 Leg. Sess. (Wash. 2021)
- California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 *et seq*.
- California Privacy Rights Act of 2020 (Cal. 2020)
- Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207
- NYDFS Circular Letter No. 2, Cyber Insurance Risk Framework (Feb. 4, 2021)
- U.S. Dep't of Treasury Office of Foreign Assets Control, Ransomware Advisory (Oct. 1, 2020)
- U.S. Securities and Exchange Commission, Cybersecurity: Ransomware Alert (July 10, 2020)
- *Data Protection Comm'r v. Facebook Ireland and Schrems*, Case C-311/18 (CJEU 2020)
- *United States v. Sullivan*, No. 3:20-cr-71168 (N.D. Cal.)
- *In re: Capital One Customer Data Security Breach Litigation*, No. 1:19-md-02915 (E.D. Va.)
- *In the Matter of Facebook, Inc.*, File No. 1910134, Dkt. No. C-4365 (FTC)/*United States v. Facebook, Inc.*, No. 19-cv-2184 (D.D.C.)
- *In the Matter of Zoom Video Commc'ns, Inc.*, File No. 1923167, Dkt. No. C-4731 (FTC)
- *In the Matter of Everalbum, Inc.*, File No. 1923172 (FTC)
- *Google LLC and YouTube, LLC*, File No. 1723083 (FTC)/*FTC v. Google LLC and YouTube, LLC*, No. 19-cv-02642 (D.D.C.)
- *Musical.ly, Inc.*, File No. 1723004 (FTC)/*United States v. Musical.ly*, No. 19-cv-1439 (C.D. Cal.)
- *In re Sabre Corp.*, No. C-702975 (La. 19th Judicial Dist.)
- *State of Washington v. Super Basic, LLC and Maple Media, LLC*, No. 20-2-01630-34 (Wash. Super. Ct. Thurston Cnty.)