Cravath Data Privacy and Security Review

H1 2023

State

CALIFORNIA PRIVACY RIGHTS ACT ENFORCEMENT UPDATE

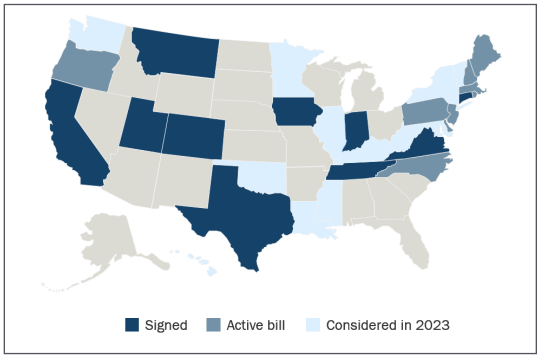
Although the substantive provisions of the California Privacy Rights Act (CPRA) took effect on January 1, enforcement has been delayed until July 1 (for provisions included in the ballot initiative) and, due to a late-breaking court ruling, March 29, 2024 (for more recently promulgated regulations).

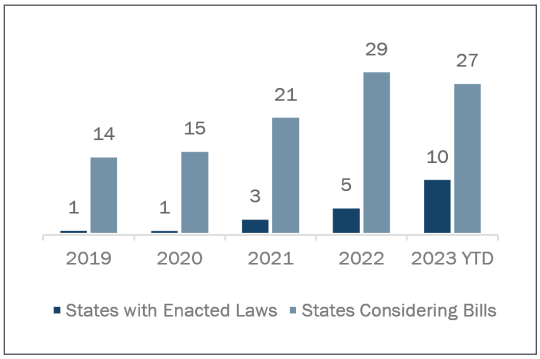
On June 30, a Sacramento Superior Court ruled that enforcement of any final California Privacy Protection Agency (CPPA) regulation under the CPRA "will be stayed for a period of 12 months from the date that individual regulation becomes final." Thus, businesses have a reprieve with respect to compliance with many of the CPRA's newest requirements—including with respect to data processing agreements, consumer opt-out mechanisms, mandatory recognition of opt-out preference signals, dark patterns and consumer request handling.

Importantly, the court's decision does not result in a complete delay of CPRA enforcement—nor does it impact the California Consumer Privacy Act (CCPA), which remains fully enforceable. Businesses must account for the sunset of key exemptions covering B2B and employee data, and must grapple with the CPRA's many other novel requirements, including its introduction of various new consumer rights, its inclusion of "sensitive personal information," a new category of information with heightened compliance requirements, and its expanded private right of action for consumers.

Notwithstanding the court's ruling, California continues to demonstrate that enforcement will be a priority moving forward. In September 2022, the California Attorney General announced the first enforcement action under the CCPA against Sephora, Inc. (Sephora) for violations of the CCPA's "Do Not Sell" provision. As part of its settlement, Sephora paid $1.2 million and is required to maintain a two-year compliance monitoring program to address CCPA and CPRA compliance. In late January 2023, California Attorney General Rob Bonta announced an "investigative sweep" of mobile applications for compliance with the CCPA's opt-out requests. In recent meetings, the CPPA has stressed its commitment to enforcement (including through hiring additional staff and technical experts), strongly suggesting that the agency is keen to act on violations when enforcement begins in earnest.

TRACKING STATE PRIVACY LAW DEVELOPMENTS





Two privacy bills were enacted in 2022, tying 2021's then-record. More than twice as many states have passed privacy laws in the first half of 2023 alone: Indiana, Iowa, Montana, Tennessee and Texas.

COLORADO AND CONNECTICUT DATA PRIVACY LAWS EFFECTIVE—AND ENFORCEABLE—JULY 1

On July 1, enforcement began for two state omnibus privacy laws: Colorado's Colorado Privacy Act (CPA) and Connecticut's Data Privacy Act (CTDPA). Like many of their enacted-but-not-effective state counterparts, the CPA and CTDPA take many of their cues from Europe's General Data Protection Regulation (GDPR), including by introducing fair information principles and establishing key data subject rights.

Applicability

To qualify as a controller under the CPA and CTDPA, an individual or entity must (i) conduct business or produce goods or services that are intentionally targeted to state residents and (ii) either: (A) control or process personal data of more than 100,000 residents per year; or (B) derive revenue from the sale of personal data of at least 25,000 residents. For Colorado, any amount of revenue suffices; for Connecticut, it must constitute 25 percent of a controller's gross revenue.

Exemptions apply for personnel and B2B information (unlike California's exemptions, which expired earlier this year). Exemptions also apply for financial institutions subject to the Gramm-Leach-Bliley Act of 1999 and institutions of higher education. The CTDPA exempts non-profits and entities subject to the Health Insurance Portability and Accountability Act of 1996; the CPA does not.

Consumer Rights

The CPA and CTDPA provide for similar consumer rights, including rights of access, correction, portability and deletion, as well as rights to limit processing and to opt out of sales of data, profiling and targeted advertising.

Opt-In Consent

Unlike many of their other state counterparts, both the CPA and CTDPA require opt-in prior consent for the processing of sensitive personal data, including data collected from children. By contrast, the CPRA does not contain an opt-in provision, but does endow consumers with the right to opt out of certain uses and disclosures of their sensitive personal data.

Enforcement; Cure Periods

In Colorado, its Attorney General and District Attorneys have enforcement authority; only the Attorney General is responsible for enforcement in Connecticut. Both states have a 60-day cure period for alleged violations, which sunset by January 2025.

NYDFS MAINTAINS FOCUS ON STRONG CYBERSECURITY ENFORCEMENT

Recent actions by the New York Department of Financial Services (NYDFS) demonstrate its continued commitment to robust enforcement of its cybersecurity regulation, 23 NYCRR Part 500 (Part 500). In early May, it fined BitFlyer USA, Inc. $1.2 million as a result of deficiencies that the agency found in the company's cybersecurity program (most notably, its failure to conduct periodic risk assessments). Later that month, it fined OneMain Financial Group, LLC $4.25 million and imposed remediation requirements on the nonprime lender's cybersecurity program.

NYDFS continues to review comments on its proposed amendments to Part 500, which address cybersecurity weaknesses identified in enforcement actions since 2019. The proposed amendments tighten requirements for all covered entities (including annual penetration testing obligations and risk assessment updates, enhanced notification requirements and others), and impose separate, more stringent restrictions on certain larger regulated entities. These amendments are expected to be finalized before year-end.

Federal

ENFORCEMENT TRENDS

Focus on cybersecurity and privacy-related enforcement at the US federal level remains heightened in the first half of 2023.

- The Federal Trade Commission (FTC) continues its trend of imposing significant penalties for privacy and cybersecurity-related violations. Consistent with Chair Lina Khan's statement that the FTC is focused on "designing effective remedies that are directly informed by" market participants' activity, this enforcement tack reflects novel approaches to monetary and nonmonetary penalties alike. In particular, the agency is seeking to trigger penalty authority by adopting rulemakings and through novel (and sometimes questionable) interpretations of statutes and rules in place today.
- The Securities and Exchange Commission (SEC) has more than doubled the size of its Crypto Assets and Cyber Unit, and remains active in data privacy- and security-related enforcement in the first half of 2023.
- The Department of Justice has also indicated that it considers cybersecurity a priority item from an enforcement perspective. Its Civil Cyber Fraud Initiative—which leverages the False Claims Act to pursue entities that provide inadequate cybersecurity products and services, misrepresent their cybersecurity practices and are deficient with respect to reporting incidents and breaches—announced its first settlement in March. The settlement resolved claims that a website developer failed to secure personal information on a federally funded children's health insurance website. In late June, the Department followed up with an announcement that it had established the National Security Cyber Section, a new litigating component within the National Security Division focused on investigating and prosecuting nation-state threat actors and their proxies involved in a range of cyber-enabled activities impacting US national security, including threats to critical infrastructure.

NOTABLE ACTIONS

- *FTC: BetterHelp, Inc., Edmodo, LLC, GoodRx Holdings, Inc.*
  Targeted advertising and children's privacy, as well as sensitive information more generally, including in the healthcare context, remain focal points for FTC enforcement.

- *SEC:* *Blackbaud Inc.*
  Increased regulatory scrutiny on cyberattacks is expected for public companies, especially in advance of the SEC's finalization of cybersecurity incident disclosure rules.[1]

TRENDING: VPPA CLAIMS MAKE A COMEBACK

The Video Protection Privacy Act (VPPA), a federal consumer privacy law that has mostly laid dormant since a flurry of litigation activity a decade ago, has once again become an active source of litigation. Since 2022, over 110 lawsuits, largely putative class actions, have been filed alleging violations of the VPPA.

The VPPA prevents the disclosure of personally identifiable information (PII) about a consumer derived from video materials or services without consent. This prohibition applies to "video tape service providers," a broad term that includes any person engaged in the delivery of video tapes "or similar audio-visual materials."

Creative plaintiffs have sought to apply the law to modern technologies allowing video files to be accessed by website visitors. They allege that website operators that use tracking tools linked to social media platforms violate the VPPA, because these websites track viewing history and share such history with the relevant social media platform.

To date, courts remain split on the issue—in particular, whether such viewing history qualifies as PII subject to the VPPA's protections. Some jurisdictions, like the Southern District of New York and the Northern District of California, have often dismissed these claims; others, like courts in Massachusetts, have denied motions to dismiss and permitted discovery. With consensus unlikely to be quickly forthcoming, expect litigation on this point to continue apace.

Global

PRIVACY BULLETIN

- May marked the fifth anniversary since GDPR came into effect. As of May 2023, nearly €4 billion in fines have been levied—of which €1.6 billion was levied in 2023 alone. As Meta grapples with the €1.2 billion fine recently levied against it in connection with its transfer of personal data to the United States and Microsoft prepares for a $425 million fine over its LinkedIn service, 2023 is poised to be a record year for enforcement. Approaches with respect to cross-border data transfers have varied among data protection authorities. As we look ahead to future enforcement, authorities' ability to harmonize with respect to the GDPR's principles will remain critical for the regulation's effectiveness.
- Businesses across the EU and US eagerly await resolution with respect to the EU-US Data Privacy Framework. The European Commission has stated that it expects the framework "to be fully functional by the summer," which would "guarantee stability and legal certainty, both sought by businesses, and would also guarantee strict protection of the private lives of citizens."
- At the end of April, in its *Single Resolution Board v. European Data Protection Supervisor* decision, the European General Court clarified that when pseudonymized information is provided without the key enabling such information to be re-identified, that information met the requirements for being anonymized and, by extension, is not subject to GDPR. Should the decision survive appeal, it will considerably ease compliance for organizations that receive only tokenized and de-identified information from EU data subjects.

1 For more information about the SEC's proposed rules, please refer to Cravath's March 17, 2022 client alert.

- Data privacy regulation continues marching forward globally. Europe's AI Act has generated real traction, and its ePrivacy Regulation, which has been in the works since 2017, continues its circuitous path forward. China's new regulations and requirements for cross-border transfers are effective. Brazil's publication of sanctions criteria under its General Data Protection Law is likely to encourage enforcement activity.

Cravath, Swaine & Moore LLP

David J. Kappos
T+1-212-474-1168
dkappos@cravath.com

Sasha Rosenthal-Larrea
T+1-212-474-1967
srosenthal-larrea@cravath.com

Evan Norris
T+1-212-474-1524
enorris@cravath.com

Noah Joshua Phillips
T+1-202-869-7740
nphillips@cravath.com

Carys J. Webb, *CIPP/US, CIPP/E*
T+1-212-474-1249
cwebb@cravath.com

NEW YORK

Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
T+1-212-474-1000
F+1-212-474-3700

LONDON

CityPoint
One Ropemaker Street
London EC2Y 9HR
T+44-20-7453-1000
F+44-20-7860-1150

WASHINGTON, D.C.

1601 K Street NW
Washington, D.C. 20006-1682
T+1-202-869-7700
F+1-202-869-7600