Cravath Data Privacy and Security Review

H2 2023

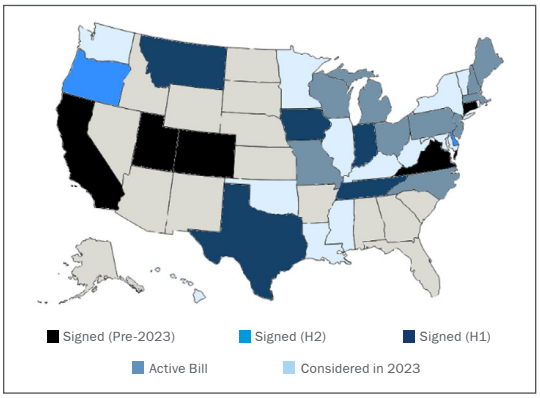
State

2023 MARKS A BANNER YEAR FOR STATE PRIVACY LAW DEVELOPMENTS

After years of a slow drip of data privacy law enactment in the US, the dam broke in 2023. Seven states enacted comprehensive privacy laws—more than double the number enacted in 2022, and more this year alone than in all other years combined. In parallel, states supplemented comprehensive laws with sector-specific privacy legislation—with multiple states passing children's privacy laws, consumer health privacy laws and data broker laws. As federal privacy legislation continues to stall out, we expect state-level activity to continue apace in 2024.

Comprehensive

State data privacy laws enacted this year (in Delaware, Indiana, Iowa, Montana, Oregon, Tennessee and Texas) share many commonalities, both in terms of definitions and overall structure. Notwithstanding this general harmony, these laws vary considerably in terms of the businesses to which they apply, the protections they offer consumers and the obligations they impose on businesses. This year's laws provide new and increasing hurdles for compliance, including: creating new consumer rights of access (Oregon); eliminating the carveout for "small businesses" (Texas); and introducing a far lower consumer threshold for applicability (Delaware). State definitions of "sensitive data" also vary, adding further complexity to the privacy compliance puzzle that businesses face.



After a record-breaking first half of 2023, where five states (Indiana, Iowa, Montana, Tennessee, Texas) passed privacy bills, the second half of 2023 was relatively subdued, with only two states passing similar bills (Delaware, Oregon).

Momentum remains high going into 2024, with some states (such as Maine and New Hampshire) carrying over bills into the new year.

Health Privacy

Washington's My Health My Data Act (MHMD) represents one of the most significant privacy laws enacted in 2023, and becomes effective starting on March 31, 2024 (June 30, 2024 for small businesses). MHMD, unlike many other generally comprehensive state privacy laws, applies regardless of an entity's revenue or the number of consumers it impacts; its "consumer health data" definition can be read expansively to cover categories not ordinarily considered health related, including certain online activity and inferences derived from non-health data; and it includes a private right of action. MHMD applies

to a broad swath of entities that collect consumer health data, but are not governed by the Health Insurance Portability and Accountability Act (HIPAA).

Other states (notably Connecticut and Nevada) enacted or amended health privacy legislation, but none of these laws is as onerous, or is likely to be as impactful, as MHMD. More activity on health privacy is expected in 2024, particularly in light of federal regulatory focus in this area.

Children's Privacy

Children's privacy was a target of much state legislative focus in 2023.

On September 18, momentum from 2022's California Age Appropriate Design Code Act (CAADC) largely stalled out when the CAADC was enjoined on First Amendment grounds. Of the seven states that considered CAADC copycat bills, none enacted any legislation.

Some states (Connecticut and Florida) found traction in children's age-appropriate design code laws that focused on data privacy controls rather than the content regulation provisions that ultimately doomed the CAADC. Other states (including Louisiana, Ohio, Texas and Utah) passed laws regulating children's use of social media, focusing on age verification and parental consent. These laws differ significantly with respect to the scope of covered companies and requirements for acceptable age verification mechanisms.

Data Brokers

On June 18 and July 27, the governors of Texas and Oregon respectively signed data broker bills into law; these states join California and Vermont in requiring data broker registration.

On October 10, California enhanced its existing data broker law through the passage of the Delete Act, which requires the California Privacy Protection Agency (CPPA) to create a "one-stop shop" for consumers to request the deletion and tracking of their personal data. Despite significant pushback from industry groups, expect a continued focus on companies that collect personal data for commercial use in 2024.

UTAH CONSUMER PRIVACY ACT GOES INTO EFFECT

On December 31, the Utah Consumer Privacy Act (UCPA) went into effect. Although it bears some similarities to its already-effective Virginia counterpart, the UCPA is the most lenient and business-friendly state privacy law on the books in terms of consumer rights granted and scope of applicability.

To come within the reach of UCPA, an individual or entity must (i) conduct business in Utah or produce a product or service that is targeted to Utah residents; (ii) have annual revenue of over $25 million; and (iii) either (A) control or process the personal data of 100,000 or more consumers per year, or (B) derive more than 50% of gross revenue from the sale of personal data and control or process the personal data of 25,000 or more consumers (effectively exempting most Utah small businesses from UCPA compliance).

Unlike other state privacy laws, Utah consumers do not have the right to correct their information, nor the right to appeal a business's denial of any UCPA request they make. There is also no private right of action under the UCPA. Additionally, Utah businesses are not required to receive affirmative consent prior to processing "sensitive data"; consent is only required in the context of processing children's information.

Although the UCPA's scope is currently narrow, Utah lawmakers have indicated its current form is only a jumping-off point for privacy regulation in the state. The Utah Attorney General and Division of Consumer Protection must report on the UCPA's effectiveness in July 2025, at which point we may see enhancements and additions to its scope.

NYDFS AMENDS PART 500

On November 1, the New York Department of Financial Services (NYDFS) finalized the second amendment to its cybersecurity regulations, 23 NYCRR 500. These amendments provide additional prescriptive requirements for covered entities with respect to cybersecurity, including enhanced access controls, expanded use of multifactor authentication and routine risk assessments. The amendments also require covered entities to report to NYDFS any ransomware and extortion payments within 24 hours of such payment.

These changes will be phased in over the next two years, with many effective as of April 2024. As NYDFS continues to take on an active enforcement role in the cybersecurity space, banks, insurance companies and the other financial services businesses under its purview should promptly review and revise their policies and procedures with these amendments in mind.

CPPA ADDRESSES CYBERSECURITY AUDITS IN DRAFT REGULATIONS AND BOARD MEETING

On December 8, the CPPA held an open Board meeting to discuss, *inter alia*, proposed regulations related to cybersecurity audits as well as risk assessments and automated decisionmaking technology (ADMT). The CPPA Board requested that CPPA staff prepare the cybersecurity audit draft regulations for final Board approval and the start of the formal rulemaking process, which includes a 45-day period for public comment.

The CPPA Board did not similarly advance the risk assessment and ADMT draft regulations, which are set to undergo further revisions and review during subsequent CPPA Board meetings.

The cybersecurity audit regulation, as currently drafted, will only apply to businesses covered by the California Consumer Privacy Act that meet certain revenue and/or information processing thresholds, and will give businesses 24 months from the effective date of the regulations to complete their first cybersecurity audit.

Federal

REGULATORY DEVELOPMENTS

SEC Cybersecurity Disclosure Requirements Start Taking Effect

On July 26, the Securities and Exchange Commission (SEC) adopted final rules regarding disclosure by public companies, including foreign private issuers, of cybersecurity risk management, strategy, governance and related incidents (Final Rules). In particular, the Final Rules require: (i) current reporting of material cybersecurity incidents; and (ii) annual reporting of companies' cybersecurity risk management process, and the roles of management and the board of directors with respect to such risks.

The Final Rules added a new Item 1.05 to Form 8-K requiring disclosure of any cybersecurity incident a company experiences that it determines to be material. The Form 8-K must be filed within four business days of the company's determination that the incident was material. The Commission included in Item 1.05 a provision that allows for delays in filing the Form 8-K if the United States Attorney General determines that the disclosure would pose a substantial risk to national security or public safety. The current Form 8-K reporting requirements for material cybersecurity incidents took effect on December 18.

One aspect of the Final Rules that was left open by the SEC was how the delayed disclosure provision would work in practice. In December, the Federal Bureau of Investigation (FBI) and Department of Justice (DOJ) joined the SEC in providing guidance on how victims of cybersecurity incidents can request a disclosure delay. Such requests must be submitted via a dedicated email address to the FBI, which will

refer the incident to the DOJ. Notably, the FBI has indicated that it will not process a request for a delay unless such request is received by the FBI "immediately" upon a company's determination to disclose a cybersecurity incident on Form 8-K. For its part, the DOJ's guidance explains that it expects the disclosure of a cybersecurity incident on Form 8-K to pose a substantial risk to national security or public safety only in "limited circumstances."

Regarding the annual reporting requirements on Forms 10-K and 20-F (for foreign private issuers), companies must describe their processes to identify, assess and manage cybersecurity risks, as well as management's role in assessing and managing, and the board's role in overseeing, such risks. The Commission did not adopt proposed requirements for disclosure of the cybersecurity expertise of individual board members, or of the frequency of board or committee discussions regarding cybersecurity. Companies must begin providing the applicable disclosures in annual reports for fiscal years ending on or after December 15, 2023.

For more information about the SEC's recently enacted cybersecurity disclosure rules, please refer to Cravath's August 1, 2023 client alert.

NIST Releases CSF 2.0 Framework

On August 8, the National Institute of Standards and Technology (NIST) released a draft of its Cybersecurity Framework (CSF) 2.0. CSF 2.0 will replace CSF 1.1, a tool designed to help organizations understand, reduce and communicate about cybersecurity risk, which was promulgated five years ago. Although originally developed for critical infrastructure, CSF—like its complement, the NIST Privacy Framework—has been leveraged across sectors and industries; the voluntary framework is widely acknowledged as the gold standard for designing cybersecurity policies and procedures. Acknowledging this broad-based applicability, NIST has stated that CSF 2.0 is designed to be "useful to all sectors, not just those designated as critical."

To that end, NIST has added governance to its core functions. According to NIST, this function is intended to flow through all other core functions and "emphasizes that cybersecurity is a major source of enterprise risk, ranking alongside legal, financial, and other risks as considerations for senior leadership." As part of this function, the CSF 2.0 framework focuses on supply chain risk management and provides more concrete implementation guidance. CSF 2.0 was open for public comment until November 6; final publication is expected in early 2024.

FTC Proposes Strengthening Children's Online Privacy Protection (COPPA) Rule

On December 20, the FTC issued a notice of proposed rulemaking (NPRM), proposing revisions to strengthen the COPPA Rule's protections and seeking comment on proposed changes. The proposed revisions include expanding the definition of "personal information" to include biometric data, strengthening data security requirements and requiring operators to obtain separate, verifiable parental consent to disclose information to third parties (unless such disclosure is integral to the nature of the operator's website or service). Once the NPRM is published in the Federal Register, the public will have 60 days to submit any comments.

FTC Finalizes Safeguards Rule Amendment

On October 27, the Federal Trade Commission (FTC) finalized its amendment to the Standards for Safeguarding Customer Information (Safeguards Rule) under the Gramm Leach Bliley Act (GLBA). The amended Safeguards Rule requires "non-banking financial institutions" to notify the FTC electronically within 30 days of

discovering a security breach where unencrypted information of more than 500 consumers is impacted, even absent risk of consumer harm. The FTC has indicated it plans to make all such reports public, and declined to provide any reporting carveout for entities subject to any other state or federal reporting obligation. The FTC has stated that publication is intended to provide an "additional incentive" to comply with the Safeguards Rule's obligations.

FCC Adopts Rules to Protect Consumers from Cell Phone Fraud Schemes

On July 11, just weeks after it was launched, the Federal Communications Commission's (FCC) Privacy and Data Security Task Force announced proposed rules to protect consumers against "SIM swapping" and port-out fraud, two forms of cell phone scams involving a victim's wireless carrier. On November 15, the FCC adopted the rules proposed by the Task Force.

CISA Finalizing Notice of Proposed Rulemaking

On September 6, Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly told an audience at the Billington Cybersecurity Summit that the agency was finishing the notice of proposed rulemaking for the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). The CIRCIA rules are expected to have broad application, as "critical infrastructure sectors" include commercial facilities, communications, financial services, food and agriculture, healthcare and public health and information technology, among others. The rules will require covered entities to report cybersecurity incidents within 72 hours, and ransomware payments within 24 hours, to CISA and the Department of Homeland Security. CISA is required to publish its notice of proposed rulemaking by March 2024 at the latest.

NOTABLE ENFORCEMENT ACTIONS

- *SEC: SolarWinds*
  On October 30, the SEC filed a complaint alleging, *inter alia*, that SolarWinds knew of the company's cybersecurity risks and vulnerabilities but misled investors regarding cybersecurity practices, and that the CISO also knew of such risks and vulnerabilities but failed to resolve or sufficiently raise them within the company. This step further reinforces the SEC's stated commitment to ensuring accurate and timely disclosures related to cybersecurity, and the agency's pursuit of individuals viewed as insufficiently addressing and/or escalating cybersecurity issues.
- *FTC: BetterHelp, Inc., 1Health.io, Easy Healthcare (Premom)*
  The FTC remains committed to leading health privacy enforcement, as evidenced by complementary enforcement actions, policy statements and regulatory activity in this space. The agency remains keenly focused on companies in the health data space, and in particular those that deal with especially sensitive health data. Enforcement actions against Betterhelp (mental health treatment data), 1Health (DNA data) and Premom (reproductive data) indicate the FTC is laying groundwork for what reasonable privacy practices are with respect to such sensitive health data and underscores its expansive reading of the Health Breach Notification Rule.
- *FTC: Rite Aid*
  In December, the FTC entered into a consent order with Rite Aid in connection with the company's use of facial recognition technology; the order is awaiting approval in federal court. The FTC alleges that Rite Aid used facial recognition technology without reasonable safeguards and failed to prevent harm to consumers, and also violated a prior FTC order pertaining to data security. The consent order will prohibit Rite Aid from

using facial recognition technology for surveillance purposes for five years.

- *HHS: L.A. Care Health Plan*
  The Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) also continues to pursue health privacy enforcement, with the largest publicly operated health plan in the country settling two OCR investigations in September 2023. The L.A. Care Health Plan investigations stemmed from two separate data breaches, and the $1.3 million settlement was the largest of the year for HHS.

PRIVATE LITIGATION

On October 4, the Judicial Panel on Multidistrict Litigation consolidated over 100 actions against Progress Software in connection with the MOVEit mass hack, perhaps the most significant cybersecurity attack of the year. Judge Allison Burroughs in the District of Massachusetts will now preside over the consolidated action. The hack of MOVEit by the Russian-linked ransomware group Clop has impacted over 2,500 organizations and over 75 million individuals, with a substantial majority of such organizations based in the U.S. More broadly, the MOVEit hack highlights the importance of reviewing and securing digital supply chains and assessing the cybersecurity practices of third and fourth parties.

Global

PRIVACY BULLETIN

Irish DPC Fine Levied Against TikTok

€345 million

On September 15, the Irish Data Protection Commission (DPC) adopted its final decision regarding its investigation into TikTok, which uncovered violations of seven articles of the GDPR. On August 3, based on the draft decision of the Irish DPC, a European Data Protection Board decision adopted an eighth violation. The Irish DPC investigation focused on TikTok's design practices in notifications shown to teens on the social media platform.

EU-US Data Privacy Framework (DPF)

2,611 active entities

On July 10, the DPF became effective, and on October 12, the complementary UK-US Data Bridge followed. It remains to be seen whether these frameworks will survive the legal scrutiny that they already face. Entities that wish to avoid concomitant risk should continue to avail themselves of alternative solutions, such as standard contractual clauses (which are themselves not entirely without risk).

For more information about the DPF, please refer to Cravath's July 13, 2023 client alert.

India's Digital Personal Data Protection Act, 2023 (DPDP Act)

₹2.5 Billion ($30 Million) Maximum Penalty Per Breach

On August 11, India's GDPR-based DPDP Act was enacted, though it has yet to come into effect and its existing requirements will be supplemented by forthcoming regulations. Unlike the GDPR, there is no revenue-based metric for penalties under the DPDP Act. The DPDP Act permits penalties of up to ₹2.5 billion per breach, but does not provide a cap on total penalties per incident—so one event could conceivably result in significant fines for offenders.

Political Agreement on EU Cyber Resilience Act (CRA)

€15 Million or 2.5 Percent, Annual Revenue Maximum Penalty for Non-Compliance

On December 1, a political agreement was reached between the European Parliament and

the Council of the European Union (Council) on the CRA, first introduced in 2022. The agreement reached is now subject to formal approval by the European Parliament and the Council. The CRA—designed to regulate products with a "digital element"—targets Internet of Things–enabled products available in the EU market.

Political Agreement on EU Artificial Intelligence Act (AI Act)

On December 9, the European Parliament and the Council reached a political agreement on the AI Act, which was first introduced in 2021. The AI Act as currently contemplated categorizes AI into four risk-based categories (minimal, high, unacceptable and specific transparency) and includes regulations tied to such risk categories. The AI Act also proposes to set up a new European AI Office to enforce and implement rules on AI, with fines for noncompliance based on a percentage of a company's global sales turnover. There is still significant time before any implementation or enforcement, however, as the language of the AI Act remains subject to finalization, and then it must be approved by EU countries and the EU Parliament before becoming law. After becoming law, the AI Act will generally take effect two years later, with certain specific provisions taking effect six months and one year post-enactment.

Trending

TRACKING PIXELS

A tracking pixel is a 1x1 pixel graphic embedded on a website or email that, like a browser cookie, is used to track user information. But unlike browser cookies, pixels can follow users across devices and advertising channels.

Tracking pixels began to draw regulators' attention at the close of 2022. In December 2022, OCR issued a bulletin warning healthcare providers of potential pixel-related HIPAA concerns. The FTC rang in the first half of 2023 with several enforcement actions against digital health companies, including BetterHelp, GoodRx and Premom, for their use of pixels.

The second half of 2023 was similarly active with respect to regulatory activity.

On July 20, OCR and the FTC jointly issued a letter to "approximately 130" hospital systems and telehealth providers, admonishing them for risks posed by unauthorized disclosure of an individual's personal health information to third parties under HIPAA. The letter specifically warned against the use of pixel tracking tools and data vulnerabilities that result from their use. In September, the FTC issued guidance echoing the July letter's HIPAA concerns and warning further of issues under the FTC Act's general prohibitions against unfair and deceptive practices.

Private litigation has developed rapidly alongside this regulatory response. Although neither HIPAA nor the FTC Act provides a private right of action, the plaintiffs' bar is pursuing new avenues for recovery. In addition to common law privacy claims, federal and state wiretap statutes remain particularly alluring for class plaintiffs, given the potential for statutory damages. But plaintiffs are getting even more inventive: at least one class action suit has used the Racketeer Influenced and Corrupt Organizations Act (RICO), which usually applies to organized crime, to argue that Meta, Alphabet and H&R Block allegedly used tracking pixels to create a "comprehensive program" to track customer information. Given the significant number of websites that employ tracking pixels, we expect additional activity—particularly for healthcare and other companies processing sensitive consumer data.

NEW YORK

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

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

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

Dean M. Nickles
+1-212-474-1135
dnickles@cravath.com

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

WASHINGTON, D.C.

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

Cravath, Swaine & Moore LLP

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