Articles + Publications | April 2023

More Privacy, Please – April 2023

WRITTEN BY

Molly S. DiRago | Ronald I. Raether Jr. | Kim Phan | James Koenig | Jessica Ring | Natasha E. Halloran | April Garbuz | Matthew R. Cali | Alexandria Pritchett | Robyn W. Lin

Editor's Note: *Iowa became the sixth state in the nation to enact a comprehensive privacy law, and California's latest privacy regulations came into effect. At the federal level, Congress experienced a leak of sensitive health data, and President Biden announced a new executive order targeting commercial spyware use by government agencies. In U.S. litigation, the Seventh Circuit held a federal labor law preempted Illinois' BIPA, the FBI and DOJ investigated TikTok, and a Meta-Cambridge Analytica settlement agreement received preliminary approval. At the international level, OECD released a report on emerging privacy enhancing technologies, Italy banned ChatGPT, and India's privacy bill received a number of amendments.*

U.S. Laws and Regulation

Iowa Governor Signs Privacy Legislation. On March 28, Governor Kim Reynold signed SF 262 into law, making Iowa the sixth state to enact a comprehensive privacy law. Effective January 1, 2025, the law mostly aligns with Utah's Consumer Privacy Act and provides for more limited consumer rights and fewer businesses requirements than other states. However, it lacks a monetary threshold for applicability like Utah (and California).

First CPRA Rules Become Effective. On March 30, the California Privacy Protection Agency announced that the California Office of Administrative Law approved the first substantive rulemaking package to further implement the California Consumer Privacy Act (CCPA). Effective immediately, these regulations purportedly harmonize existing CCPA regulations with California Privacy Rights Act (CPRA) amendments.

Biden Executive Order Prohibits U.S. Government Use of Commercial Spyware. On March 27, President Biden signed an executive order (EO), prohibiting the use of commercial spyware that poses significant counterintelligence or security risks to the United States or poses risks of improper use by a foreign government or foreign person. Commercial spyware includes vendor-sold cyber surveillance tools that access electronic devices remotely, extract user content, and manipulate user components — all without the users' knowledge or consent. The EO applies to U.S. federal agencies, while also directing new reporting and information sharing requirements within the executive branch to ensure agencies can make informed and consistent determinations.

Colorado Finalizes its Privacy Act Rules. On March 15, 2023, the Colorado Attorney General's office finalized its Colorado Privacy Act (CPA) Rules making Colorado the third state, after California and Virginia, to enact a general state privacy law and the second to draft related rules. The Rules clarify an entity's obligations to comply with the CPA enacted in 2021. The Rules regulate the processes and disclosures of data controllers and their processors, including expectations for notices and consumers' data rights. Specifically, the Rules detail obligations and expectations for consumer disclosures (Part 3), consumer personal data rights (Part 4), universal

opt-out mechanisms (Part 5), duties of controllers (Part 6), consumer consent (Part 7), data protection assessments (Part 8), and consumer profiling (Part 9). Both the CPA and Rules will go into effect on July 1, 2023.

Cyberattack Leaks Sensitive Congressional and Staff Data. On March 9, a cyberattack on Washington, D.C. health care platform DC Health Link resulted in the leak of Social Security numbers, home addresses, and other personal data belonging to Congress members, staff members, and their spouses and dependent children. An online hacking forum claimed that hackers stole a database containing information belonging to 170,000 people. DC Health Link confirmed the breach and will notify affected individuals to offer free credit monitoring services. House Speaker Kevin McCarthy (R-CA) and Minority Leader Hakeem Jeffries (D-NY) believe that thousands of House members and employees have used DC Health Link since 2014, so the size and scope of the impacted House customers could be "extraordinary."

SEC Advances Three Cybersecurity Rules. On March 15, the Securities and Exchange Commission (SEC) proposed new rules to address cybersecurity risks in the U.S. securities market. The first proposal would require SEC-registered brokers, dealers, investment companies, and investment authorities to adopt written policies and procedures to address unauthorized access to, or use of, customer information. The second proposal would require certain entities (*e.g.,* broker-dealers, clearing agencies, and national securities associations) to address cybersecurity risks through policies and procedures, notify and report cybersecurity incidents to the SEC, and publicly disclose such incidents to improve transparency. The third proposal would expand the scope of entities subject to regulations systems compliance and integrity, bringing within its scope registered security-based swap data repositories, exempted clearing agencies, and certain large broker-dealers.

Washington House Passes Reproductive Health Bill. On March 4, the Washington House of Representatives passed House Bill 1155, which would protect reproductive health data, while also prohibiting the sale of consumer health data not protected under Health Insurance Portability and Accountability Act (HIPAA). It also would require consumer consent before sharing or collecting personal, health-related data. The bill now sits in front of the Senate.

Senators Seek to Prevent Using Health Data for Advertising. On March 6, U.S. Senators Amy Klobuchar (D-MN), Elizabeth Warren (D-MA), and Mazie Hirono (D-HI) introduced the Upholding Protections for Health and Online Location Data (UPHOLD) Privacy Act (S. 631), designed to prevent the use of personally identifiable health data for commercial advertising. The bill would place additional disclosure restrictions on companies using personal health information without user consent and bans the sale of precise location data. The bill denotes the latest in a series of actions by agencies and lawmakers aimed at protecting personal health data from misuse.

U.S. Litigation and Enforcement

Labor Law Blocks Unionized Workers' Illinois BIPA Claims. Following the Seventh Circuit's precedent in *Miller v. Southwest Airlines Co.* and *Fernandez v. Kerry, Inc.*, on March 23, the Illinois Supreme Court held that the federal Labor Management Relations Act preempts the state's Biometric Information Privacy Act (BIPA) in a claim brought by union-represented employees. Plaintiff William Walton argued that the Illinois Supreme Court should have departed from the federal precedent because the Seventh Circuit fundamentally misunderstood the consent that BIPA requires from individuals participating in a company's biometric data collection practices. The court deferred to the uniform federal case law, finding that when an employer invokes a broad management rights

clause from a collective bargaining agreement in response to a BIPA claim brought by bargaining employees, "it is both logical and reasonable" to hold that any dispute between them be resolved according to federal law and their agreement. As a result, Walton must go before an adjustment board, instead of a court, to pursue claims against Roosevelt University for unlawfully collecting and using his scanned fingerprint data.

Telehealth Company Shares Patient PII With Advertisers. On March 10, Cerebral, Inc., a telehealth tech startup that attests to providing affordable and convenient mental health services, issued a HIPAA privacy breach notification, admitting to inadvertently sharing private health information with advertisers and social media platforms, including mental health assessments of more than 3.1 million patients in the United States. The type of information affected by the disclosure included patient names, phone numbers, email addresses, birth dates, IP addresses, insurance information, appointment dates, and treatment plans. Affected individuals can contact Cerebral to learn more about the disclosure.

FBI and DOJ Investigate TikTok's Spying on Journalists. The Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) launched an investigation against TikTok parent company ByteDance for accessing the locations of American journalists and other private user data through the app. In December 2022, ByteDance confirmed that employees used TikTok to surveil journalists and other U.S. citizens. According to sources, the FBI conducted interviews related to the surveillance. In addition, the DOJ Criminal Division and the U.S. attorney for the Eastern District of Virginia subpoenaed ByteDance for information related to the spying events. It remains unclear if the DOJ's subpoenas relate to the FBI's interviews, but both agencies comprise part of the Committee on Foreign Investment in the United States (CFIUS), which recently demanded that ByteDance divest from TikTok or face a nationwide ban of the app.

Meta-Cambridge Analytica Deal Receives Preliminary Approval. On March 28, District Judge Chhabria tentatively signed off on a $725 million class-action settlement involving Meta and Cambridge Analytica. The class, composed of all Facebook users in the U.S. between May 2007 to December 2022, is estimated at 250 to 280 million people. The lawsuit concerned March 2018 allegations that a third-party app developer took personal data from Facebook users and sold it to Cambridge Analytica.

$1.75M Deal In School Software Data Breach Gets Final Nod. On March 3rd, a California federal judge granted final approval for a $1.75 million deal requiring Aeries Software, Inc. to compensate almost 100,000 individuals who had an Aeries account through their school district at the time of a data breach. The breach occurred in November 2019, when 166 databases hosted on Aeries' servers were subjected to unauthorized access, however, Aeries did not notify its school district customers until April 2020. Plaintiffs accused Aeries of failing to adequately safeguard personal identifying information such as students' health care records, social security numbers, grades and standardized test information, as well as financial information belonging to parents and guardians. Individual settlements have been made for affected individuals outside of the San Dieguito Union High School District class action. Additionally, Aeries will offer all settlement class members 12 months of credit monitoring to mitigate post-exposure risk of identity-related fraud.

International Regulation and Enforcement

Italian Data Protection Authority Bans ChatGPT. On March 31, the Italian Data Protection Authority (Garante) announced a ban on popular chatbot ChatGPT and launched an investigation into whether its provider OpenAI

violated the GDPR. The Garante alleged OpenAI failed to inform users and individuals that it collected and processed their personal data to train the algorithm of its data processing practices. It also accused OpenAI of failing to check ChatGPT users' ages to ensure that it did not collect information from children.

India's Digital Data Protection Bill Undergoes Amendments. On March 28, members of India's Parliament on the Parliamentary Standing Committee on Information Technology proposed 40 amendments to the draft Digital Data Protection Bill. The committee's concerns included the lack of autonomy of the proposed Data Protection Board, blanket exemptions given to some data fiduciaries, and a lack of attention to protecting children's data. There is no clear timeline when the committee will introduce the bill to Parliament.

OECD Releases Report on Emerging Privacy-Enhancing Technologies. On March 31, the Organisation for Economic Co-operation and Development released a report on emerging privacy-enhancing technologies (PET). The report reviewed recent technological advancements and evaluated the effectiveness of different types of PETs. The report also outlined current regulatory and policy approaches to help enforcement authorities understand how these technologies can enhance privacy and data protections.

Troutman Pepper Team Spotlight: Cindy Hanson

Cindy focuses her practice on class-action defense, having handled more than a thousand matters under the Fair Credit Reporting Act, including hundreds of class actions. She represents consumer reporting agencies, entities furnishing information to consumer reporting agencies, employers using background check information for employment purposes, and data brokers, among others. Further, Cindy leverages her extensive experience in successfully defending companies in class actions under consumer protection statutes and state common law.

In her spare time, you can find Cindy — and avid New York Yankees fan — watching her twin boys playing baseball, one a catcher and the other a pitcher/outfielder.

Upcoming Webinars, Podcasts, and Events

- Alan Wingfield, Kim Phan, and Jack Altura (Speakers), "Who's Watching the Watchers? – A New Wave of Website Litigation Webinar," April 19, 2023
- RSA Conference, San Francisco, April 24-27
- Privacy + Security Forum Spring Academy, May 10-12, Washington, D.C.
- NetDiligence Cyber Risk Summit, Philadelphia, May 31-June 2

Past Webinars, Podcasts, and Events

- IAPP Global Privacy Summit 2023, April 4-5, Washington, D.C.
- Kamran Salour and Sadia Mirza (Speakers) and Surefire Cyber Chief Delivery Officer Joseph Tarraf (Guest), "Unauthorized Access Podcast," Troutman Pepper, April 6, 2023
- Chris Miller and Tom Dwyer (Speakers), "SAAS Roundtable: Attracting and Retaining Top Talent," Boomi, March 3, 2023
- Shelli Willis (Speaker), "An Investment In Climate – How The SEC Climate Disclosure Could Accelerate Decarbonization," UPS, February 28, 2023

Recent Troutman Pepper Publications

- FCRA Ruling Boosts Technical Claim Defense
- Illinois: BIPA – the 'Gold Standard' of Biometric Legislation
- Iowa on Cusp of Enacting Privacy Legislation
- Did You Suffer a Data Breach and What Are Your Notice Obligations?
- Cyber Capsule – February 2023

Interested in comprehensive legislative and regulatory tracking services focused on consumer financial services? Troutman Pepper offers weekly reports on developments in consumer collection, consumer reporting/FCRA case law, and privacy and data security. Contact Stefanie Jackman (stefanie.jackman@troutman.com), Kim Phan (kim.phan@troutman.com), or Michael Bevel (michael.bevel@troutman.com) for more information and to request a free trial.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management