Articles + Publications | February 2023

More Privacy, Please – February 2023

WRITTEN BY

Molly S. DiRago | Ronald Raether, Jr. | Matthew R. Cali | April Garbuz | Natasha E. Halloran | Jessica Ring | Kim Phan | Robyn W. Lin | Alexandria Pritchett | Graham T. Dean | Joshua D. Davey

Editor's Note: *As the nation celebrated National Privacy Day on January 28, in regulatory news, the Colorado AG published a third version of its proposed regulations, and the CPPA voted to submit its draft regulations to the Office of Administrative Law. In litigation, the SEC sought records from law firm Covington and Burling, and Whole Food agreed to a BIPA settlement. In international news, Slovenia's new Personal Data Protection Act came into force.*

U.S. Laws and Regulation

- **President Biden Highlights Privacy During State of the Union Address.** During his State of the Union address, President Biden spoke about children's privacy rights and improving data privacy protection. He called for bi-partisan cooperation among lawmakers to improve protections. The House is currently considering the American Data Privacy Protection Act (ADPPA), which the House Energy and Commerce Committee marked up in 2022.
- **CPPA Begins Additional Rulemaking.** The California Privacy Protection Agency issued an invitation for preliminary comments on proposed rulemaking on cybersecurity audits, risk assessments, and automated decision-making topics. The invitation asked several questions including:

• What existing laws require cybersecurity audits and risk assessments, and what processes have companies implemented to comply with such laws?

• How are specified terms, such as "automated decision-making," currently defined under other laws, and should the CPPA adopt such definitions?

• What impact has rulemaking made on both businesses and consumers?

• Preliminary comments will be accepted from February 10 through March 27.

- **CPPA Takes Next Step to Promulgating Regulations.** The California Privacy Protection Agency (CPPA) voted unanimously in favor of submitting the current draft California Privacy Rights Act (CPRA) regulations (published on January 31) to California's Office of Administrative Law (OAL). Once formally submitted, the OAL must approve or disapprove the regulations in 30 business days. Per California's administrative law, the CPPA also released a draft "Economic and Fiscal Impact Statement" and the "Final Statement of Reasons" for the final CPRA regulations. Based on this timeline, the proposed regulations could take effect as early as April, therefore, businesses should start implementing compliance efforts now.
- **Colorado Publishes Third Draft of Privacy Regulations.** On January 27, the Colorado attorney general (AG) released a third version of the proposed draft rules. This draft of regulations removed the requirement that controllers must notify consumers of substantive changes to the privacy notice. The latest draft also removed the 15-day requirement imposed on opt-out requests in favor of a requirement that businesses comply "without

undue delay." On February 1, the Colorado Department of Law held a meeting for comment on the draft regulations.

- **FCC Issues Notice of Proposed Rulemaking for Data Breach Notification.** On January 5, the Federal Communications Commission (FCC) issued a notice of proposed rulemaking (NPR) on data breach notifications that impact customer proprietary network information (CPNI) — information that telecommunications companies acquire about their subscribers, including services subscribed to, current charges, directory assistance charges, usage data, and calling patterns. The NPR proposed removing the mandatory seven-day waiting period before notifying consumers, while suggesting a "without unreasonable delay" standard. The NPR also proposed expanding the definition of a "breach" to include inadvertent, but harmful data disclosures.
- **States Introduces More Comprehensive Privacy Laws and Privacy Protections for Minors.** Numerous states introduced comprehensive privacy legislation: Iowa (SSB1071), Kentucky (SB15), New Hampshire (SB255 and HB314) New Jersey (A505), New York (S3162, S365, and A1366), Oklahoma (HB1030), Oregon (SB619), Tennessee (SB73), Vermont (H121), and Washington (HB1616). Several states introduced 2023 legislation focused on the privacy of minors: Connecticut (HB6393), New Jersey (S3493), and West Virginia (HB2460).
- **California AG Focuses on Mobile Apps for Data Privacy Day.** On January 27, California Attorney General Rob Bonta announced an "investigative sweep" of businesses with mobile apps that allegedly failed to comply with consumer requests to stop the sale of their personal information. Released just ahead *Data Privacy Day* on January 28, the AG's announcement noted that the sweep focused on popular apps in the retail, travel, and food industries, including on requests submitted through the *Consumer Reports* application Permission Slip, which allows consumers to submit request to opt out and delete their information. This announcement denoted the most recent step taken by the California AG's office to enforce the CCPA. For more information, click here.
- **HHS Settles HIPAA Investigation With Arizona Hospital System.** On February 2, the Department of Health and Human Services' Office for Civil Rights (OCR) announced a settlement with Banner Health Affiliated Covered Entities (Banner Health) — a nonprofit health system that suffered a data breach in 2016. The incident disclosed the protected health information of 2.81 million consumers. The settlement under HIPAA's Security Rule included a $1.25 million fine and implementing a corrective action plan.
- **NY AG Settles With CEO of Spyware Companies.** On February 2, New York AG Letitia James announced a $410,000 settlement with Patrick Hinchy's 16 companies, which all sold spyware that allows a user to monitor another person's device without their knowledge. The investigation also revealed that Hinchy's companies misrepresented their refund and data security policies and failed to disclose the potential harm to a device when installing the software. Consequently, the settlement mandated that Hinchy's companies must alert device owners that their devices are being monitored and required accurate disclosures on data security and jailbreaking requirements for software installation.
- **NY AG Investigates Madison Square Garden's Use of Facial Recognition.** On January 24, New York AG Letitia James sent a letter to the Madison Square Garden Entertainment Corporation, seeking information about its use of facial recognition technology to prohibit ticketholders from entering their venues. The letter arose after the corporation used facial recognition software to identify and prohibit several attorneys from entering Radio City Music Hall.

U.S. Litigation and Enforcement

- **Court Orders Covington to Show Cause for Alleged Noncompliance With SEC Cyberattack Subpoena.** On January 24, a federal judge issued an order, directing Covington & Burling LLP to show cause why the court should not compel its compliance with a March 21, 2022 SEC subpoena that sought information about 298 of Covington's clients impacted by the law firm's 2020 cyberattack. Specifically, the SEC requested "information about impacted parties and the extent of that impact," such as "the names of any clients whose information had been viewed, copied, modified or exfiltrated during the attack on Covington." The SEC asked for this information to investigate "the impact of the Cyberattack on public companies and regulated entities in order to (a) understand the nature and scope of the attack, (b) assess and identify potential illegal trading based on information gathered during the attack, and (c) determine relevant disclosure obligations for public companies impacted by the attack." In response, Covington argued that attorney-client privilege protected the firm from providing this confidential information.

- **Meta Prevails Over Injunction Enjoining Pixel Use.** On December 22, 2022, Judge William Orrick denied the plaintiffs' motion for injunctive relief after they alleged Meta improperly acquired their protected health information through the Meta Pixel installed on their health care providers' patient portals. They argued that by logging into the patient portal, the Meta Pixel transmitted certain information to Meta. Judge Orrick held that while the plaintiffs demonstrated a likelihood of succeeding on the merits, they failed to meet the threshold of demonstrating that the balance of equities tips in their favor. Judge Orrick also ruled that several unknowns affected his ability to make a judgment on equities, including how many hospitals used the Meta Pixel, how Meta filtered information, and the amount of data that was filtered through by Meta.
- **Foot Locker Faces Lawsuit Over Alleged CIPA Violations for "Eavesdropping" Through Virtual Chat Features.** On January 23, plaintiff Ruth Martin filed a putative class action against Foot Locker in the Northern District of California, alleging Sections 613 and 632.7 violations of the California Invasion of Privacy Act (CIPA) by "covertly wiretap[ping] the personal conversations" of customers using the chat feature available at footlocker.com. The plaintiff claimed that Foot Locker's chat feature automatically records and transcribes all conversations initiated by customers and then allows "at least one" independent third-party vendor to secretly intercept the chat communications. Although the plaintiff named Smooch and Zendesk as the potential independent third parties, she failed to allege how she discovered the alleged violation. The plaintiff instead asserted that as a consumer advocate, she has an interest in Foot Locker's product offerings, and as a "tester," she works to "ensure that companies … abide by the strict privacy obligations imposed under California Law."
- **Whole Foods Agrees to Pay $300K for Recording Warehouse Workers' Voices.** On January 3, a preliminary order was entered, requiring Whole Foods to pay out nearly $300,000 in a class-action settlement in possibly the first voiceprint settlement under Illinois' Biometric Information Privacy Act (BIPA). At the Chicago warehouse, employees receive a headset to track assignments. The system works by identifying an employee's voice patterns as it gives commands, however the plaintiff alleged that the system captured employees' "voiceprints" without their consent. The plaintiff contended that those voiceprints constitute biometric data like fingerprints, and Whole Foods should have provided employees with information on how it kept and treated their voiceprints under BIPA. According to the complaint, Whole Foods did not first ask for their employees' consent; employees never received a written policy on the use of their biometric identifiers, nor did Whole Foods ever tell employees when their voiceprints would be deleted from the grocery store's systems.
- **Class Action Against Twitter Claims 200M Compromised Accounts.** On January 13, Twitter user Stephen Gerber filed a putative class action in the Northern District of California against Twitter, Inc., arising from an alleged data breach that resulted in the unauthorized collection of Gerber's personal information. Gerber alleged hackers obtained his personal information via a defect in Twitter's application programming interface, which allowed cybercriminals to scrape data between July 2021 and January 2022. Gerber also claimed that he found information taken from more than 200 million Twitter accounts on an internet hacker website. In a blog post, Twitter insisted that no evidence existed "that the data recently being sold online was obtained by exploiting a vulnerability of Twitter systems," and the information the hackers obtained likely came from data already publicly available through various online sources.
- **Assurance IQ Shakes Website Activity Tracking Suit.** On January 5, a California federal judge dismissed as untimely a proposed class-action lawsuit against an insurance website operator and its software provider. Under the CIPA, plaintiffs must bring their claims within one year of the violation; the statute of limitations begins tolling when a plaintiff has "knowledge of the injury." The judge found that the plaintiff was on notice of a potential violation at least as early as January 2019 (16 months before he filed his April 2020 class action) but gave leave for the plaintiff to amend his claims.
- **Pennsylvania Wiretap Suit Alleges Apple Tracks Users Who Opt Out.** On January 6, a proposed class action was brought against Apple in the Eastern District of Pennsylvania, alleging that the company unlawfully recorded and used consumers' personal information and activity on mobile devices and apps, even after consumers indicated through device settings that they did want their data and information shared. The class could conceivably contain hundreds of thousands of consumers in Pennsylvania who had their information collected by Apple after turning off "Allow Apps to Request to Track," "Share iPhone Analytics," or similar settings on an Apple mobile device. The complaint cited a recent report, claiming that Apple still collects information on its users through the App Store on its devices, even after turning off the tracking setting. The suit sought financial compensation for the company's alleged violation of Pennsylvania's Wiretapping and Electronic Surveillance Act and Pennsylvania Unfair Trade Practices and Consumer Protection Law, while also

alleging invasion of privacy, breach of implied contract, and unjust enrichment claims. A similar suit over Apple's data collection practices was filed in California federal court in November 2022, alleging more CIPA violations.

- **Yodlee Wants Judge to Rethink Early Win in Privacy Suit.** On January 6, financial data aggregator Yodlee, Inc. asked U.S. Magistrate Judge Sallie Kim to reconsider her decision to partially deny summary judgment on fraud claims against the company, asserting that the court misinterpreted California law relating to damages. In August 2020, the plaintiffs sued Yodlee and its parent company Envestnet, Inc., claiming Yodlee violated users' privacy rights and mishandled their data, leaving them vulnerable to fraud and identity theft. In Yodlee's motion to reconsider, it argued that the court's finding that the plaintiffs could not establish any cognizable damages for fraud meant the plaintiffs also could not establish damages for an unjust enrichment claim.
- **Michigan College Hit With Third Class Action After Data Breach.** On January 5, the owner of a landscaping company filed the third class-action lawsuit against private liberal arts college Hope College for failing to take adequate measures to protect personal information possibly exposed in a 2022 data breach. The plaintiff, who had done business with the college, contended Hope College should be held liable for the breach — which potentially disclosed the names, dates of birth, student ID numbers, driver's license numbers, and Social Security numbers of up to 150,000 people — because the school failed to encrypt the stored data or follow routine cybersecurity procedures. The complaint alleged breach of implied contract, unjust enrichment, and negligence, naming "everyone affected by the breach" as putative class members. Two other class-action lawsuits were filed in late December 2022 shortly after Hope College notified affected parties of the potential breach.
- **Otonomo Obtains Motion to Dismiss in Vehicle Tracking Suit.** On January 18, Judge Thompson granted Otonomo's motion to dismiss a class action, alleging the company surreptitiously tracks drivers' locations and movements through electronic devices installed in their cars. The plaintiffs sued under the CIPA, alleging the company placed internet-connected devices in BMW vehicles. Judge Thompson held that the statute prohibited placing an electronic tracking device on a vehicle by an unregistered owner. Since the telematics control unit at the heart of the allegations was built into the car, the unit was already owned by the same registered owner. Judge Thompson also ruled that the complaint lacked allegations that Otonomo obtained personal information of the drivers, rather than only collecting vehicle locations. She also ruled that the plaintiff failed to allege that he did not consent to the tracking.

International Regulation and Enforcement

- **Slovenia's Personal Data Protection Act Becomes Effective.** On January 26, Slovenia's Personal Data Protection Act — adopted on December 15, 2022 — went into effect. The law regulates "transmission of personal data in the public and private sector," biometrics, and "personal data processing for research, archival and statistical purposes."
- **EU Council and EU Parliament Reach Agreement on Access to E-Evidence.** On January 25, the EU member states' confirmed an agreement between the council presidency and the European Parliament on draft regulations and draft directive on cross-border access to e-evidence. This will allow relevant authorities to address judicial orders for electronic evidence directly to service providers in another member state.
- **EDPB Publishes Decision on the Legal Basis of Processing for Behavioral Advertising.** On January 12, the European Data Protection Board (EDPB) published its decision to force the Irish Data Protection Commission to reverse a 2021 conclusion, as well as its finding that Meta's practice of using consent to engage in behavioral advertising through a claim of contractual necessity is unlawful.
- **WhatsApp Incurs $5.9M Fine for GDPR Violations.** On January 20, the Ireland Data Protection Commission (DPC) fined WhatsApp $5.9 million in a matter arising out of its May 25, 2018 "terms of service" update. The DPC's investigation concluded that WhatsApp breached its GDPR transparency violations because users had "insufficient clarity as to what processing operations were being carried out on their personal data." Notably, the DPC also stated the GDPR did not preclude WhatsApp's reliance on the assertion that the new "terms of use" constituted a contract. Six of the DPC's 47 peer regulators disagreed with this aspect of the judgment, and because a consensus could not be reached, the DPC referred the issue to the European Data Protection Board.

Troutman Pepper Spotlight: Tricia Brauer

As legal counsel and a strategic business advisor to Fortune 50 and Fortune 100 companies, startups, and investment funds, Tricia Brauer operates at the intersection between technology and real estate, intellectual property and licensing, and cross-border privacy regulations. In her daily work, she is called upon to counsel business teams and C-suite executives alike on a wide range of commercial matters, including mergers and acquisitions, joint ventures, technology transactions and agreements, and smart infrastructure and sustainability initiatives. Tricia's career is rich and varied, with exposure to private law firms, as well as in-house for public companies. This mix of Big Law and in-house experience enables her to excel in providing practical and proactive legal advice in a way that aligns with a company's internal business processes and strategy, while mitigating risk.

Fun Fact: After being approached in an New York City coffee shop, Tricia and her husband Nick accepted an invitation to audition for a popular Netflix reality series on planning a wedding/buying a house. After making it to the final round, the show ultimately selected another couple because Tricia and Nick "liked each other too much" and "weren't dramatic enough." Rejection never felt so sweet!

Upcoming Webinars, Podcasts, and Events

- Shelli Willis (Speaker), "An Investment In Climate – How The SEC Climate Disclosure Could Accelerate Decarbonization," UPS, February 28, 2023

Past Webinars, Podcasts, and Events

- Kim Phan (Speaker), "Federal Data Privacy & Security Update," RMAi, February 8, 2023
- Sadia Mirza and Kamran Salour (Speakers), "All the Questions You've Wanted to Ask About Cyber Insurance but Were Afraid to Ask," Troutman Pepper, February 13, 2023
- David Anthony (Speaker), "Breakout B: Litigation Update," NetDiligence Cyber Risk Summit, February 21, 2023
- Sadia Mirza and Kamran Salour (Speakers), "Unauthorized Access Podcast: Inside the Mind of Lynn Peachey," Troutman Pepper, February 22, 2023

Recent Troutman Pepper Publications

- The Safeguards Rule: Protecting Information at Financial Institutions
- Preparing for an Era of Regulated Artificial Intelligence
- Troutman Pepper's Interactive Incident Response Map
- CFPB's Involvement in Tenant Screening
- What We Learned From 2022's Top FCRA Developments
- Bonta Issues New Investigative Sweep of Mobile Application Companies
- Illinois holds five-year limitations period applies to all BIPA claims

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management