More Privacy, Please – August/September 2023

WRITTEN BY

Molly S. DiRago | Natasha E. Halloran | Ronald Raether, Jr. | James Koenig | Kim Phan | Karla Ballesteros | April Garbuz | Robyn W. Lin

Editor's Note: As the summer months come to an end, there has been no shortage of privacy news and updates. Oregon signed both a comprehensive privacy law and data broker law, and the SEC adopted new rules regarding the disclosure of cybersecurity incidents. Online tracking technologies continue to be a source of both regulatory concern and litigation, with the FTC and HHS jointly sending a letter to hospitals about online tracking and numerous companies grappling with wiretapping claims. Internationally, India finally passed a comprehensive privacy law, and several data protection authorities issued a joint statement on data scraping.

U.S. Laws and Regulation

California AG Targets Employee Data. California Attorney General (AG) Rob Bonta recently announced that his office sent inquiry letters to large California employers requesting information regarding their California Consumer Privacy Act (CCPA) compliance with respect to employee and job applicant personal information. This latest investigative effort asks covered California employers to demonstrate how they are complying with the legal obligations set forth in the CCPA, including individuals' rights to access, delete, and opt out of the sale and sharing of personal information. The investigative sweep follows a similar announcement in January 2023 targeting mobile applications and their compliance with the CCPA.

Oregon Adds Data Broker Law. On July 27, Oregon Governor Tina Kotek signed HB 2052 into law, requiring data brokers to register with the Department of Consumer and Business Services. Effective January 1, 2024, businesses that register must identify whether consumers have any opt-out rights with respect to the business' collection, selling, or licensing activities, and if so, the method of opt out. The law provides for a civil penalty of up to $500 per day for violations.

Oregon Governor Signs Comprehensive Privacy Law. On July 26, Kotek signed SB 619 into law. Unlike other state privacy laws, the bill requires controllers to provide consumers with a list of specific third parties to whom their personal data was disclosed. It excludes not-for-profit businesses for the first year and does not apply to employee or business-to-business (B2B) data. Additionally, the bill contains complicated exemptions of personal health information and certain data that is collected or processed in accordance with financial laws, such as the Gramm-Leach-Bliley Act. The act will take effect on July 1, 2024 (July 1, 2025, for nonprofits).

SEC Adopts Cybersecurity Rules. On July 26, the Securities and Exchange Commission (SEC adopted a final rule by a 3-2 margin, to require more immediate disclosure of material cybersecurity incidents by public companies. In addition, the final rule requires annual disclosure of material information regarding a public company's cybersecurity risk management strategy and cybersecurity governance. For cybersecurity events

determined to be material, Form 8-K must be filed within four business days of the materiality determination.

CPPA Announces Investigation Into Connected Vehicles. On July 31, the California Privacy Protection Agency (CPPA) announced a review of data privacy practices by connected vehicle (CV) manufacturers and related CV technologies. In its announcement, the CPPA described CVs as "connected computers on wheels," explaining that they collect consumers' location information and support smartphone integration among other technologies. CPPA Executive Director Ashkan Soltani stated the CPPA would be seeking to "understand how these companies are complying with California law when they collect and use consumers' data."

FTC and HHS Caution Against Use of Online Tracking Technologies. On July 20, the Federal Trade Commission (FTC) and U.S. Department of Health and Human Services' Office for Civil Rights (OCR) sent a letter to 130 companies, including hospitals, HIPAA-covered entities, telehealth providers, and health app developers, warning that, while sometimes beneficial, online tracking technologies pose privacy and security concerns. The letter states that such tracking technologies gather identifiable information about users, often without their knowledge, and that it is difficult for consumers to avoid such technology when interacting with a website or mobile app.

U.S. Litigation and Enforcement

Bumble's Motion to Dismiss under Illinois BIPA Rejected in Federal Court. On July 7, U.S. District Judge Andrea R. Wood denied Bumble's motion to dismiss for lack of personal jurisdiction in a class action lawsuit alleging the company violated the Illinois Biometric Information Privacy Act (BIPA) by failing to inform Illinois users that it collected and maintained their biometric information through the app's optional photo verification feature. Judge Wood rejected Bumble's arguments that the app did not target Illinois residents specifically, holding that Bumble "purposefully availed itself of the Illinois market for its dating app services by deliberately and continuously exploiting that market." Judge Wood cited Bumble's advertising on physical billboards, hosting happy hour events in Chicago, sponsoring booths at Chicago's Lollapalooza festival, and employing campus ambassadors at universities in Chicago in support of her decision. Judge Wood also held that Bumble's entities collectively are "multi-million-dollar entities with global reach," which does not support a finding of unfairness.

Ninth Circuit Affirms TCPA Ruling. On August 8, a unanimous Ninth Circuit affirmed a district court's partial dismissal in *Trim v. Reward Zone USA LLC*, which held that text messages were not "artificial or prerecorded voices" under the Telephone Consumer Protection Act (TCPA) because they did not include audible components. The class action complaint alleged that the plaintiff had received at least three mass marketing text messages using prerecorded voices in violation of the TCPA. While the TCPA does not define "artificial or prerecorded voice," the Ninth Circuit employed traditional tools of statutory construction and held that Congress intended 'voice' to encompass only audible sounds.

California Court Dismisses Wiretapping Suit Against Papa John's. On August 14, a California district court dismissed a class action against Papa John's, alleging the pizza chain unlawfully tracked visitors to its website in violation of California's Invasion of Privacy Act (CIPA). CIPA prohibits the use of a recording device to intercept or eavesdrop on confidential communications without the consent of all parties. Judge Dana Sabraw dismissed the action, holding that the plaintiff was unable to "plead around the key defect that defendant cannot be liable for eavesdropping on its own conversation."

MeTV Wins Dismissal of VPPA Suit. On July 6, a federal district court in Illinois dismissed a Video Privacy Protection Act (VPPA) case due to the plaintiffs' failure to state a claim. In *Gardener v. MeTV*, the plaintiffs filed a class action suit alleging that defendant MeTV knowingly disclosed their personal video viewing history and associated unique Facebook User ID to Meta without their consent in violation of the VPPA. The court dismissed the case, agreeing with MeTV that plaintiffs failed to plead they met the definition of a consumer under the law.

Court Dismisses VPPA Case Against NBA for Failure to State Claim. On August 7, a federal district court granted the National Basketball Association's (NBA) motion to dismiss for failure to state a claim under the VPPA. Relying on *Carter v. Scripps Networks, LLC*, the court held that the plaintiff was not a "subscriber" under the VPPA because he had the same access to videos on the NBA.com site as any other visitor, and while he also subscribed to the NBA's newsletter, there were no allegations that the newsletter subscription allowed him unique access to videos. The court also held that even if the newsletter contained a link directing users to video content, links to content that is generally accessible to the public are "insufficient to create a subscriber relationship."

Court Defers VPPA Case to Summary Judgment. On July 28, the Northern District of California partially denied Bleacher Report Inc.'s motion to dismiss claims brought under the VPPA, excepting only those claims based on live streaming videos. While the plaintiff had not explicitly alleged that the videos at issue were pre-recorded, the court held that, read in the light most favorable to the plaintiff, his claims raised the inference that Bleacher Report provided pre-recorded video content. The court also rejected Bleacher Report's argument that a nonparty, Facebook, collected the user data through its pixel tracking tool, finding adequate allegations that Bleacher Report collected the information. The court distinguished the case from *Martin v. Meredith Corporation,* explaining that the alleged disclosure in *Martin* was limited to the name of a webpage that contained a video, not the name of the video itself.

Health Company Settles Class Action Pixel Suit for $12.25M. On August 21, the Eastern District of Wisconsin granted the plaintiff's unopposed motion for preliminary approval of the parties' class action settlement in *In Re Advocate Aurora Health Pixel Litigation*. Per the agreement, Advocate Aurora Health will pay $12.25 million to resolve class claims that the company shared users' protected health information without consent to third parties like Meta and Google through a tracking pixel embedded on its website, app, and patient portal. Filed on May 5, the class action complaint asserted 11 causes of action against Advocate Aurora Health, including claims for invasion of privacy intrusion upon seclusion and publication of private facts, unjust enrichment, breach of implied contract, breach of confidence/professional negligence, and violations of the Electronic Communications Privacy Act, Wisconsin's Deceptive Trade Practices Act, and Illinois' Consumer Fraud and Deceptive Business Practices Act. In addition to the $12.25 class fund, the company agreed to implement remedial fixes to ensure its tracking pixel usage materially complies with HIPAA. The court set a final approval hearing for March 8, 2024.

Health System Faces Breach of Contract Claim Based on Privacy Disclosures. On August 22, a federal district court denied UCSF Medical Center's motion to dismiss after the plaintiff amended her breach of contract claim to allege she had received or otherwise sufficiently assented to UCSF's Health Notice of Privacy Practices Act or Website Privacy Statement. The plaintiff's breach of contract claim arises out of three contracts: (1) Terms and Conditions for UCSF MyChart, (2) UCSF website Terms of Use, which incorporate by reference the Privacy Policy Statement, and (3) UCSF Notice of Privacy Practices. The court found the amended complaint "'clearly alleged' the bases for contractual duties that UCSF has breached, as well as how those contractual provisions were communicated to plaintiff," including UCSF's disclosure on the MyChart login page. The court noted that the

plaintiff's claim did not seek to require compliance with legal duties under HIPAA or California's Confidentiality of Medical Information Act, but instead based her claims on privacy and data sharing promises made by UCSF that extend beyond such statutory duties.

CPPA Appeals CPRA Regulation Injunction. On August 4, the California Privacy Protection Agency (CPPA) and California AG Rob Bonta announced they had filed an appeal with California's Third District Court of Appeals. Previously, the Sacramento County Superior Court had enjoined the CPPA from enforcing the most recently promulgated CCPA regulations based on the California Privacy Rights Act of 2020 (CPRA). These regulations were promulgated on March 29, almost nine months after the deadline provided in the statute.

NYC Bans TikTok. New York City is prohibiting the use of TikTok on government devices, giving city agencies 30 days to remove the app and banning employees from downloading or using TikTok on city-sanctioned tech. This decision was prompted by concerns from NYC Cyber Command about TikTok posing a security threat to the city's technical networks. It follows a similar ban by New York state in 2020. While some states have banned TikTok more broadly, most have restricted its use for government employees only. ByteDance, the company behind TikTok, continues to defend itself against claims that it is a national security threat.

BIPA Fingerprinting Class Certified. On August 22, an Illinois federal judge ruled that Rich Products Corp. must face a proposed class action alleging the improper storage of employees' fingerprints in violation of the BIPA. The judge denied the food supplier's motion to dismiss the suit reasoning it is not time-barred or preempted by the Illinois Workers' Compensation Act based on recent rulings by the Supreme Court of Illinois. The judge also rejected arguments that the plaintiff lacked standing and that the complaint did not meet the plausibility standard. The case, originally filed in 2018, centers around the collection of biometric information through fingerprint timekeeping without proper consent.

International Regulation and Enforcement

EU-US Data Privacy Framework Finalized. On July 17, the EU-U.S. Data Privacy Framework was finalized and went into immediate effect. This comes after the director of national intelligence confirmed that all U.S. intelligence agencies have adopted implementing procedures as required by Executive Order 14086 on Enhancing Safeguards for U.S. Signals Intelligence Activity and the adoption of the adequacy decision by the European Commission.

India Passes Personal Data Protection Bill. On August 9, Indian lawmakers passed a comprehensive data privacy bill, the Digital Personal Data Protection Bill (DPDPB). Like other international privacy laws, DPDPB introduces principles for data processing, mandates stricter consent requirements, and provides individuals with rights to access, correct, and erase their personal data. DPDPB proposes penalties of up to 2.5 billion rupees ($30 million) for violations and noncompliance. The government has not yet announced when the DPDPB will take effect.

Data Protection Authorities Issue Joint Statement Regarding Web Scraping. On August 24, 12 data protection authorities including those from Australia, Canada, the United Kingdom, Hong Kong, Norway, Switzerland, and Mexico, issued a joint statement on data scraping and the protection of privacy. The statement emphasized that personal information that is publicly accessible is still subject to various data privacy laws and

that companies hosting publicly available information still have obligations under these legal regimes. The statement also included a reminder that mass data scraping incidents can constitute a reportable data breach under various legal regimes and encouraged individual users to take steps to protect their personal information.

Troutman Pepper Team Spotlight: Gene Fishel

Richmond Counsel Gene Fishel brings extensive regulatory experience to Troutman Pepper, having most recently served as senior assistant attorney general and chief of the Computer Crime Section in the Office of the Attorney General of Virginia, and as special assistant U.S. attorney in the Eastern District of Virginia for 20 years.

As a regulator, Gene has reviewed thousands of database breach incidents and investigated hundreds of cybersecurity, privacy, and consumer protection violations, including as part of multistate attorneys general teams. He has been a pillar in the charge for sweeping reforms to privacy and computer crime laws, having drafted and shepherded dozens of successful bills involving database breach notification, electronic records, identity theft, computer trespass, and child exploitation statutes, among others. In his supervisory capacities, he led the professional development of attorneys and computer forensic examiners, overseeing more than 1,000 prosecutions and computer forensic investigations for complex criminal cases in Virginia.

In 2015, Gene, was in Los Angeles to give a talk in his former capacity with the attorney general's office. Having a day to kill in the City of Angels, he attended a taping by himself of The Price is Right. Much to his surprise, he was selected to "come on down" at the show's beginning, bid correctly to get on stage, and then won the game, the prize being a trip to Buenos Aires! While his wife was unable to be at the taping, they did enjoy a remarkably inexpensive trip to Argentina.

Upcoming Webinars, Podcasts, and Events

- Troutman Pepper and Innovation Shipyard Alliance (Hosts), CISO/CSO/General Counsel Summit, September 15, 2023.

Past Webinars, Podcasts, and Events

- Stephen Piepgrass, Ron Raether, and Dave Gettings (Speakers), "AI: Impact and Use in Background Screening ," Troutman Pepper, June 7, 2023.
- Jim Koenig, Kim Phan, Joshua Davey, Sadia Mirza, Jack Altura, and Robyn Lin (Speakers), "Privacy Parade: How to Navigate the Rush of New State Privacy Laws," Troutman Pepper, June 22, 2023.
- Jim Koenig, Peter Wakiyama, and Kim Phan (Speakers), "Navigating the AI Landscape: Privacy, IP, Policies and More – An Industry Expert Roundtable," Troutman Pepper, July 20, 2023.
- Kim Phan, Chris Willis (Speakers), "Recent Developments in California Privacy Laws," Troutman Pepper, July 27, 2023.

- Tracey Diamond, Evan Gibbs, and Alison Grounds (Speakers), "The Pros and Cons of Generative AI in the Workplace: The Matrix," Troutman Pepper, August 9, 2023.

- Jason Lichter, Alison Grounds, Tracey Diamond, Ashley Hager, Kim Phan, Jim Koenig (Speakers), "Artificial Intelligence – From Risk to Reward: Key Questions to Address When Crafting Generative AI Usage Policies," Troutman Pepper, August 21, 2023.

- Ethan Ostroff, Dave Gettings, Kim Phan, Chris Willis (Speakers), "CFPB's Rulemaking Under the FCRA – Crossover Episode with FCRA Focus Podcast," Troutman Pepper, September 7, 2023

Recent Troutman Pepper Publications

- Data Protection: One of These Incidents Is Not Like the Other

---

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.

Ben Duwve, a 2023 summer associate with Troutman Pepper who is not admitted to practice law in any jurisdiction, also contributed to this newsletter.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management