

More Privacy, Please – January 2024

WRITTEN BY

Molly S. DiRago | Ronald I. Raether Jr. | Kim Phan | James Koenig | Natasha E. Halloran | Linnea J. Kelly | Safvet T. Besen | Robyn W. Lin

Troutman Pepper recently published its [2023 Privacy Year in Review](#), a comprehensive analysis of the year's key developments in privacy, security, and artificial intelligence, which offers practical advice for companies navigating the bewildering number of virtual threats and technological advancements. This annual guide to global trends, risks, best practices, and detailed case studies is a collaborative effort of our Privacy + Cyber and Regulatory Investigations, Strategy + Enforcement (RISE) teams. It aims to serve as a vital resource to help companies address current cybersecurity, privacy, and data protection challenges and prepare for future ones.

Editor's Note: *In recent regulatory and enforcement developments, New Jersey became the latest state to enact a comprehensive privacy law, and the Connecticut Attorney General released the first report on CTDPA. The FTC entered into two privacy consent decrees, both of which centered on the sale of sensitive location data. In litigation, VPPA and wiretapping litigation continues to surge, including a denial of a motion to dismiss filed by Hearst. Internationally, the EU member nations unanimously voted to pass the AI Act, a Canadian government agency experienced a data breach, and the French data protection authority fined a data broker for failing to comply with GDPR.*

U.S. Laws and Regulation

NIST Publishes Report on the Cybersecurity of Genomic Data. On December 20, 2023, the NIST National Cybersecurity Center of Excellence (NCCoE) published [Final NIST IR 8432, Cybersecurity of Genomic Data](#). Informed by direction from Congress, this report discusses current practices, challenges, and potential solutions for securing genomic data. Based on this report's findings, NCCoE has developed [Draft NIST IR 8467, Cybersecurity Framework \(CSF\) Profile for Genomic Data](#), which provides actionable guidance to organizations that process genomic data to help these organizations manage and protect against cybersecurity risks. NCCoE is also in the process of developing a Privacy Framework Profile for Genomic Data to supplement the CSF. This Privacy Framework Profile will be publicly released later in 2024.

FTC Reaches First Data Broker Settlement. On January 9, the FTC reached its first settlement with a data broker involving the alleged collection and sale of location information that could be used to track individuals' visits to places of worship, reproductive health clinics, and domestic abuse shelters. Under the [proposed order](#), X-Mode Social, Inc. and its successor Outlogic, LLC will be prohibited from sharing or selling such data going forward. For a deeper analysis by our team, click [here](#).

FTC Bans InMarket Media's Sale of Precise Location Data. On January 18, the FTC [announced](#) another enforcement action focused on the collection and use of consumers' sensitive location information. The FTC

entered into a consent order with InMarket Media for the use or sale of the precise location data it collects for marketing and targeting advertising. InMarket Media must also provide an “easy-to-find way” for consumers to withdraw their consent to location data collection and for the ability to request the deletion of previously collected data. This proposed administrative complaint and consent decree is open for public comment until February 17.

Iowa AG Brings Suit against TikTok. On January 17, Iowa AG Brenna Bird filed a [complaint](#) in the Polk County District Court, alleging TikTok misrepresented that access to inappropriate content on its app by children is “infrequent.” In its description on Apple’s app store, TikTok is labeled as an app for individuals aged 12 and above with “infrequent/mild” access to inappropriate content. However, Bird alleges that, “[t]he TikTok app contains frequent and intense sexual content and nudity, profanity and crude humor, mature and suggestive themes, and alcohol, tobacco, and drug use and references.” TikTok has already been subject to scrutiny by other U.S. governmental authorities for ties to China and the app’s data and child safety measures.

U.S. Litigation and Enforcement

ReproSource Fertility Reaches Breach Settlement. On January 10, Massachusetts fertility test center ReproSource Fertility Diagnostics (a Quest Diagnostics company) [reached a \\$1.25 million settlement](#) resolving negligence claims related to an August 2021 ransomware attack that impacted approximately 350,000 patients. Although ReproSource cut off network connection immediately after discovering the unauthorized activity, threat actors were able to gain access to patients’ names, email addresses, dates of birth, and protected health information (PHI) like CPT and diagnosis codes, health insurance billing information, and physician information. Affected individuals were not notified until October 2021. Plaintiffs in the ensuing class action litigation alleged that ReproSource was negligent in failing to safeguard patient information, especially as health care organizations like ReproSource are frequent cyberattack targets. Plaintiffs also noted that ReproSource failed to notify impacted individuals within 60 days, as required by HIPAA for PHI breaches. The settlement allows class members to submit claims of up to \$3,000 as reimbursement for out-of-pocket losses. Since the breach, ReproSource claims it has adopted more advanced data security measures, including additional cybersecurity measures, at its own expense.

Burger King Franchisee Says Insurance Carrier Owes Defense Costs for BIPA Suit. In a [lawsuit filed](#) on January 17, Burger King franchisee Tri City Foods Inc. (Tri City) claims that its insurance carrier owes the franchisee coverage for a class action alleging violations of Illinois’ Biometric Information Privacy Act (BIPA). The underlying class action was initiated in 2018 by a former employee of Tri City who claimed that Tri City tracked his time worked by requiring him to scan his fingerprint at the beginning and end of each shift. The plaintiff alleged that Tri City violated BIPA by failing to inform him of any biometric data retention policy and failing to obtain a written release for the collection and storage of his fingerprints. This underlying action remains ongoing.

Hearst’s VPPA Claim Continues. On January 11, a judge [denied](#) a media company’s motion to dismiss a putative class action under the Video Privacy Protection Act (VPPA). The plaintiffs allege that the company disclosed their personally identifiable information (PII), including a record of every video they viewed on Hearst’s mobile applications, to third parties in violation of the VPPA. The court found that the plaintiffs plausibly alleged that they were consumers, the company was a video tape service provider, and that there was a knowing transmission of PII, as defined under the statute. The court also found that the plaintiffs did not need to plead actual damages and may proceed without alleging any specific pecuniary loss. Further, the court rejected the

company's argument that the ordinary course of business exception applies because the alleged uses of plaintiffs' information (marketing, advertising, and analytics) does not fall within the exception's narrow list of permissible uses. Lastly, the court found that the allegations involve commercial speech, so the VPPA satisfies the intermediate scrutiny test in accordance with the First Amendment.

Carnival's Wiretap and Invasion of Privacy Claims Proceed. On January 19, a judge [granted in part and denied](#) in part, defendant Carnival Corporation's motion to dismiss plaintiffs' federal and state wiretap and invasion of privacy claims. Plaintiffs allege that the travel company enlists third-party companies to embed session replay software on its website, which collects information about the user's system and "all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry (even if deleted), and numerous other forms of a user's navigation and integration through the website." The court found the company's argument that it provided the consumers notice of its recording policy through a cookie policy banner displayed at the bottom of its website and that consumers assented to the terms of that policy through their continued use of the website to be premature. Specifically, the court noted that the banner's text is smaller than the rest of the bolded large text on its homepage and the company has not demonstrated that the banner appears immediately or that it persists for a user's entire visit. Thus, the court held that the plaintiffs plausibly alleged the interception of their communications without consent. However, the court dismissed the Consumer Fraud and Abuse Act claim without prejudice because plaintiffs' allegations of damage or loss were entirely conclusory.

Fidelity National Financial Reveals Data Breach Affected 1.3M Consumers. Insurance company Fidelity National Financial Inc. [revealed](#) it suffered a cyberattack in November that affected 1.3 million consumers. Ransomware gang ALPHV (or BlackCat) claimed responsibility for the attack in a post on its dark web leak site. At this time, Fidelity is providing credit monitoring and identity theft restoration services to consumers after also reporting it was hit with several lawsuits in the wake of the attack.

Papa John's Faces Putative Class Action in California Web Tracking Suit. Popular pizza chain, Papa John's, was unable to dismiss in full a class action lawsuit, alleging the pizza chain illegally tracked users' online activity on its website. The court [held](#) that plaintiffs adequately alleged that Papa John's had violated the California Invasion of Privacy Act (CIPA). Papa John's was successful, however, in dismissing the plaintiff's bid for injunctive relief as well as claims that the company had intercepted telephone communications under CIPA. The court found that there was no threat of future harm for injunctive relief and that CIPA applied only to communications between two certain types of telephones, not the internet, which the complaint failed to allege. The claims were dismissed with leave to amend.

International Regulation and Enforcement

EU Members Unanimously Vote to Advance the AI Act. On February 2, EU Members [reached a political agreement](#) on the Artificial Intelligence (AI) Act (the Act). Two parliamentary committees (the internal market and civil liberties committees) will vote on February 13 and a full plenary vote is expected either April 10 or 11. The Act will create new rules and obligations for providers and users of AI depending on the level of risk from AI. The Act will ban unacceptable risks, such as social scoring or biometric identification, and will require other AI, such as generative AI to comply with transparency requirements. Once adopted, the AI Act will enter into force 20 days after publication. The AI Act contains several application dates, including those for high-risk AI systems and prohibited AI Systems.

Canadian Government Agency Experiences Data Breach. On January 30, Global Affairs Canada announced an “unplanned IT outage” to address the discovery of malicious cyber activity. The Canadian Broadcasting Corporation (CBC) [reported](#) that an internal email stated that the internal systems were vulnerable between December 20, 2023 and January 24, 2024. Global Affairs Canada manages diplomatic and consular relations, promotes Canadian international trade, and leads Canada’s international development and humanitarian assistance.

French Data Protection Authority Fines Data Broker €75,000. On January 30, the Commission Nationale de L’informatique et des Libertés (CNIL) announced it had fined data broker Tagadamedia €75,000. During the investigation, the CNIL discovered Tagadamedia failed to comply with the obligation to have a legal basis for processing data and that the forms used by the company failed to provide consumers with free, informed, and unambiguous choices. The CNIL also stated that Tagadamedia’s record of processing activities was shared with a second company, but the record of processing activity did not specify which company was acting as a data controller.

Troutman Pepper Team Spotlight: Sadia Mirza

Sadia was recently promoted to partner in the firm’s Privacy + Cyber practice, effective January 1. Located in the firm’s Orange County office, she leads the firm’s Incidents + Investigations team, advising clients on all aspects of data security and privacy issues.

She is the first point of contact when a security incident or data breach is suspected, and plays a central role in her clients’ cybersecurity strategies.

She dedicates her practice to counseling clients on complex data security and privacy issues. Capitalizing on her extensive experience guiding clients through security incidents, she handles pre-incident planning and readiness, breach investigations, and litigation matters. Sadia leverages her 360-degree knowledge of the incident response

lifecycle to ensure clients can present a positive and defensible narrative to plaintiffs or regulators.

An active and respected voice in the privacy and data security bar, she writes and speaks frequently on trends and developments affecting clients and consumers. Sadia has been a panelist on numerous privacy and cybersecurity panels across the U.S. and is a member of the Program Committee for the Law Track for the RSA Conference.

Sadia provides ongoing analysis and commentary on developments in the consumer financial services industry, with a focus on privacy law, through the *Consumer Financial Services Law Monitor* blog at cfslawmonitor.com. She frequently publishes in *Bloomberg Law* and *Law360*.

Upcoming Webinars, Podcasts, and Events

- Sadia Mirza (Panelist), "[Evolution in Crisis Communications & Public Relations](#)," NetDiligence CyberRisk Summit, Miami, FL, February 13, 2024.

Past Webinars, Podcasts, and Events

- Kim Phan (Speaker), "[2023 Data Privacy & Security Roundup](#)," Receivables Management Association Annual Conference, February 7, 2024.
- Sadia Mirza (Speaker), [Unauthorized Access Podcast: "Snooping Sadia Talks to Former Official Gene Fishel"](#), Troutman Pepper, January 31, 2024.
- Sadia Mirza (Speaker), [Unauthorized Access Podcast: "Ross is Boss"](#), Troutman Pepper, January 10, 2024.
- Chris Willis, Kim Phan (Speakers), [The Consumer Finance Podcast: "SEC's New Cyber Rules for Publicly Traded Companies"](#), Troutman Pepper, December 21, 2023.
- Chris Willis, Dave Gettings, Kim Phan, Ron Raether, (Speakers), [FCRA Focus Podcast: "New Developments in the CFPB's FCRA Rulemaking Process – What's Next?"](#) Troutman Pepper, December 7, 2023.

Recent Troutman Pepper Publications

- [Navigating the Complexities of Regulatory Data Incident Investigations](#)
- [Trans Union Settles for \\$15 Million with CFPB and FTC Over Tenant Screening Reports](#)
- [Online Tracking Case Dismissed by Ninth Circuit Holding That Online Purchase Does Not Subject Web-Based Payment Processing Platform to Personal Jurisdiction in California](#)
- [FTC Amends Safeguards Rule to Require Reporting of Data Breaches](#)
- [California Takes an Aggressive Approach to Regulating Data Brokers](#)
- [California Delete Act: An Aggressive Approach to Regulating Data Brokers](#)
- [Your Organization has Suffered a Data Incident: Now Here Are the Regulators It Will Likely Encounter](#)

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

- [Business Litigation](#)
- [Privacy + Cyber](#)
- [eDiscovery + Data Management](#)