Articles + Publications | February 2024

More Privacy, Please – February 2024

WRITTEN BY

Molly S. DiRago | Natasha E. Halloran | Ronald Raether, Jr. | James Koenig | Kim Phan | Linnea J. Kelly | Karla Ballesteros | Susie Lloyd | Edgar Vargas | Safvet T. Besen | Robyn W. Lin

Editor's Note: *In recent regulatory and enforcement developments, the White House announced a new executive order aimed at strengthening cybersecurity at U.S. ports, and another executive order was issued to protect sensitive personal information. Additionally, the FCC prohibits using AI to clone voices. Data breach litigation continues to surge with one company striking a class action settlement agreement with payments of up to $75,000 per class member. In an interesting twist, the beauty company L'Occitane is suing a law firm seeking declaratory judgment that California's wiretapping law is unconstitutional. Internationally, the Canadian government investigates a breach of its own agency, and ASEAN and the EU published a joint guide on cross-border contractual clauses.*

U.S. Laws and Regulation

White House Announces EO to Protect Sensitive Personal Data. On February 28, the White House announced an executive order (EO) authorizing the attorney general (AG) to prevent large-scale transfer of Americans' personal data to countries of concern and provide safeguards around other activities that give those countries access to Americans' sensitive data. The EO identifies genomic data, biometric data, personal health data, geolocation data, and financial data as examples of personal and sensitive information and directs the Departments of Justice, Homeland Security, Health and Human Services, Defense, and Veteran Affairs to take action to safeguard this data. The EO is meant to address the president's worry that commercial data brokers and companies will sell this data to countries of concern, which will end up in the hands of foreign intelligence services, militaries, or companies controlled by foreign governments.

FCC Prohibits AI Voice Cloning Technology. On February 8, the Federal Communications Commission (FCC) announced the unanimous adoption of a Declaratory Ruling confirming that calls made with artificial intelligence (AI)-generated voices are "artificial" under the Telephone Consumer Protection Act (TCPA). The TCPA restricts telemarketing calls and the use of automatic telephone dialing systems and artificial or prerecorded voice messages. This ruling now makes it illegal to use AI-generated voice messages in robocalls without complying with the TCPA requirements, such as obtaining prior express consent. According to the FCC, this action is "expanding the legal avenues through which state law enforcement agencies can hold these perpetrators accountable under the law." The ruling takes effect immediately.

White House Announces EO on Cybersecurity at US Ports. On February 21, the Biden-Harris administration unveiled an EO detailing a $20 billion investment to enhance the security of U.S. port infrastructure. This order empowers the U.S. Coast Guard with express authority to counteract malicious cyber activities within the nation's Marine Transportation System (MTS). It also mandates the reporting of cyber incidents or imminent cyber threats

that pose a risk to any vessel, harbor, port, or waterfront facility. The U.S. Coast Guard has subsequently released a Notice of Proposed Rulemaking concerning cybersecurity in the MTS. The Proposed Rule is designed to strengthen the security of the interconnected network of ports, terminals, vessels, waterways, and land-side connections that make up the MTS. It does this by setting forth minimum cybersecurity standards that align with international and industry-recognized standards.

GAO Says Homeland Security Failed to Disclose AI Use in Cybersecurity Programs. On February 7, the Government Accountability Office (GAO) reported that the U.S. Department of Homeland Security (DHS) has not complied with a presidential EO to maintain an inventory of all AI use cases. The GAO found that DHS had inaccurately labeled at least one program as using AI, when in fact it did not. As a result, the GAO concluded that the DHS was not in full compliance with the GAO's 2021 AI Framework for federal agencies to responsibly design, develop, deploy, and monitor AI systems.

FTC Publishes Blog Post on Potential UDAAP Violations for Policy Updates. On February 13, the Federal Trade Commission (FTC) published a blog post warning that if a company adopts more permissive data practices — for example, it starts using personal data for AI training — that are not identified in its privacy policies, making retroactive amendments to its terms of service or privacy policy may not be enough. It could be deemed an unfair or deceptive practice if the company does not specifically notify customers. For more information, visit our summary, here.

New York AG Enters Consent Order with College Board. On February 13, New York State Education Department (NYSED) Commissioner Betty A. Rosa and New York AG Letitia James announced a $750,000 settlement with College Board for alleged violations of the privacy of students and unlawfully licensing their data to colleges, scholarship programs, and other customers who used it to solicit students. In addition to this settlement, College Board is prohibited from monetizing New York student data that it acquires from New York schools and school districts.

U.S. Litigation and Enforcement

Government Agencies Are Not Immune from FCRA Liability. On February 8, the U.S. Supreme Court unanimously ruled that government agencies can be sued for violations of the Fair Credit Reporting Act (FCRA). A borrower secured a loan from a division of the U.S. Department of Agriculture (USDA) and later sued the agency for damages under the FCRA. The borrower alleged that the USDA inaccurately reported his loan as "past due," damaging his credit score and ability to secure loans at affordable rates. The USDA argued it was immune from such suits and the district court agreed. However, the Supreme Court affirmed the Third Circuit's reversal of the district court's ruling, holding that the FCRA allows for suits against "any person," including government agencies. The reasons: the FCRA's statutory text captures government agencies as potential defendants. For more information, click here.

HHS Resolves Insider Cybersecurity Investigation for $4.75M. On February 6, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR), announced a $4.75 million resolution with a nonprofit hospital system related to potential data security failures that allowed an employee to steal and sell patients' protected health information (PHI) over a six-month period. In May 2015, the New York Police Department informed the medical center that there was evidence of theft of a certain patient's medical information. The incident prompted

the medical center to conduct an internal investigation, revealing that an employee stole the electronic PHI of 12,517 patients and sold the information to an identity theft ring. The medical center filed a breach report with OCR and the OCR investigated. The investigation revealed multiple potential violations of the Health Insurance Portability and Accountability Act's (HIPAA) Security Rule, including failures by the medical center to analyze and identify potential risks and vulnerabilities to PHI, monitor and safeguard its health information systems' activity, and implement policies and procedures that record and examine activity in information systems containing or using PHI. In addition to paying $4.75 million, the medical center must implement a corrective action plan that identifies certain steps toward protecting and securing the security of PHI.

Dad Sues Hacked Chicago Children's Hospital Again. On February 9, a plaintiff already suing Ann Lurie Children's Hospital in Chicago, IL over alleged negligence in the hospital's management of medical records, filed an additional class action complaint against the hospital. The new complaint alleges that the hospital failed to secure and safeguard the plaintiff's and class members' private information, including names, birth dates, addresses, and medical and treatment information. According to the complaint, current and former patients' private information was exposed following a cybersecurity attack in January. The complaint alleges that the hospital confirmed that its network had been accessed by a "known criminal actor." The plaintiff alleges that the hospital failed to properly audit and monitor its IT systems and vendors, causing its system to be vulnerable to this cyberattack. In addition to monetary damages, the suit seeks injunctive relief to "prevent [the hospital] from experiencing another [] cybersecurity breach by adopting and implementing best data security practices to safeguard Private Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft."

Missouri Hospital Faces Action Over Breach Of 500K Patients' Data. On February 13, a Missouri resident filed a class action complaint against North Kansas City Hospital alleging that the hospital took five months to notify more than 500,000 patients that their sensitive information was compromised in a hacking event that occurred between March and May of 2023. The complaint states that Perry Johnson & Associates, a Nevada-based medical transcription service used by North Kansas City Hospital, notified the hospital that the data breach had exposed the personal information of 502,430 patients on July 21, 2023. The hospital did not notify these patients of the breach until January 3, 2024. The complaint alleges that by waiting until January to notify the affected patients, the hospital violated its own privacy policies. In addition, the complaint states that "defendants knew, or should have known, that the information they collected was a target for malicious actors," but "despite such knowledge, defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect plaintiff's and class members' PII/PHI from cyber-attacks that defendants should have anticipated and guarded against." The medical transcription service is also the subject of several other proposed class actions in various states following large-scale data breaches in 2023 that impacted more than 3.9 million patients.

ParkMobile Users Request Class Certification in Data Breach Litigation. Parking app company, ParkMobile, is being sued by consumers alleging that inadequate cybersecurity measures by the company led to their data being stolen, sold, and given away for free on the dark web after a 2021 data breach. On February 13, the plaintiffs sought certification of the class. The plaintiffs allege that more than 20 million users' full names, birthdates, passwords, cellphone numbers, and vehicle information are among the stolen information. The consumers have requested that a Georgia federal judge certify their class.

Connexin Software Strikes Deal Over Breached Info. On February 14, plaintiffs and Connexin Software announced a $4 million settlement over allegations of failing to properly safeguard the personal identifiable information of more than 200,000 patients, including children, after a data breach. The settlement also includes a commitment from Connexin to strengthen their data and information security measures, and an agreement that Connexin will pay each plaintiff (i) up to $75,000 for any out-of-pocket losses incurred from the breach, (ii) identity theft protection for up to three years, or (iii) a flat fee.

L'Occitane Files Suit Against Law Firm for CIPA Allegations. On February 9, L'Occitane, Inc., filed a complaint in the Central District of California, seeking declaratory judgment and injunctive relief against the law firm Zimmerman Reed LLP and 3,144 of Zimmerman's clients, asserting that the law firm and its clients impermissibly manufactured thousands of claims against L'Occitane under the California Invasion of Privacy Act § 630 *et seq*. (CIPA). L'Occitane is challenging the constitutionality of CIPA, alleging it violates the First Amendment of the U.S. Constitution as an unlawful content restriction on speech and as being void for vagueness, and argues in the alternative that CIPA is preempted by the Communications Decency Act, 47 U.S.C. § 230. In support of its argument that CIPA is unconstitutional, L'Occitane cites the Ninth Circuit's recent finding that Oregon's wiretapping law was unconstitutional. *Project Veritas v. Schmidt*, 72 F.4th 1043 (9th Cir. 2023). L'Occitane also seeks declaratory relief that L'Occitane's terms and conditions do not apply to the defendants, as more than 90% of Zimmerman's purported clients allegedly have never placed an order on L'Occitane's website, a minimum requirement for the terms and conditions to apply to create a binding contract between L'Occitane and its customers.

International Regulation and Enforcement

OPC Announces Data Breach Investigation. On February 26, the Canadian Office of the Privacy Commissioner of Canada (OPC) announced an investigation into a data breach at the government agency, Global Affairs Canada. The investigation comes after the OPC received several complaints about the matter and will examine the adequacy of safeguards in place to protect personal information and compliance with the Privacy Act.

Flows of Data to Shanghai to Be Relaxed. On February 7, Reuters reported that the Shanghai government will accelerate approval for foreign firms wanting to send their local data offshore. This acceleration would happen under a fast-track approval initiative. To accomplish this, Shanghai will likely leverage its free trade zone, which allows local governments to offer tax and other incentives to global companies. These rules would be separate from the Cybersecurity Administration of China's rules on cross-border transfer of data.

Publication of Joint Guide on ASEAN Model Clauses and EU Standard Contractual Clauses. On January 31, the Association of Southeast Asian Nations (ASEAN) and the EU released a joint guide detailing how to navigate the model contractual clauses and the standard contractual clauses. These are optional clauses that can be incorporated into contracts as a basis to allow the transfer of personal data across borders. The guide provides a comparison of both sets of clauses as well as implementation guides for companies to consider best practices when operationalizing the contractual clauses.

Troutman Pepper Team Spotlight: Molly DiRago

Molly S. DiRago
Partner
Chicago
D 312.759.1926
molly.dirago@troutman.com

Molly DiRago, a partner at Troutman Pepper specializing in Business Litigation and Privacy + Cyber practices, has been honored as one of the Notable Women in Law for 2024 by Crain's Chicago Business. Molly focuses her practice on complex business disputes and privacy litigation and compliance. As a member of the Northern District of Illinois' trial bar, she represents and advises her clients in every phase of litigation with an eye toward trial. She has a nationwide practice, having represented clients in state and federal courts across the U.S. Her clients range from large, multinational companies to small, closely held corporations and individuals, spanning a variety of industries, including technology, agriculture, health care, solar, transportation, and energy.

Past Webinars, Podcasts, and Events

- Peter Wakiyama (Speaker), "Troutman Pepper Legal Operations Summit," Troutman Pepper Horizons Series, March 6, 2024.
- Jim Koenig (Speaker), "FTC Privacy Enforcement," Georgia Bar Association 38th Annual Privacy & Technology Law Conference, March 6, 2024.
- Jim Koenig (Speaker), "Navigating the Generative AI Landscape in Health Care and Life Sciences," Association of Corporate Counsel March 5, 2024.
- Laura Hamady (Speaker), "Cross Border Data Transfers," Georgia Bar Association 38th Annual Privacy & Technology Law Conference, March 5, 2024.
- Mac McCullough (Speaker), "International Privacy Law – India, China, Japan, Brazil," Georgia Bar Association 38th Annual Privacy & Technology Law Conference, March 5, 2024.
- Dave Gettings, Kim Phan, Cindy Hanson, Ron Raether, (Speakers), FCRA Focus Podcast: "CFPB Advisories on Background Checks and File Disclosures" Troutman Pepper, February 20, 2024.
- Sadia Mirza (Panelist), "Evolution in Crisis Communications & Public Relations," NetDiligence CyberRisk Summit, Miami, FL, February 13, 2024.
- Kim Phan (Speaker), "2023 Data Privacy & Security Roundup," Receivables Management Association Annual Conference, February 7, 2024.
- Peter Wakiyama (Speaker), "Innovation in Technology," Emerald Asset Management Investment Forum, February 1, 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

- California AG Announces Second CCPA Settlement, Asserting DoorDash Failed to Deliver Privacy
- Troutman Pepper Forms Incidents + Investigations Team | Troutman Pepper
- Final Rule Aligns 42 CFR Part 2 with HIPAA and HITECH
- That’s a Wrap…or Not? Regulatory Data Incident Investigation Resolutions and the Path Forward
- New York: NYDFS further enhances its cybersecurity regulations
- The Garden State Joins the Privacy Policy
- 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