Articles + Publications | May 2023

More Privacy, Please – May 2023

WRITTEN BY

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

Editor's Note: *Indiana became the latest state to enact a comprehensive privacy law, with Montana and Tennessee close behind. Washington passed sweeping legislation — the My Health My Data Act — which included a private right of action. At the federal level, the CFPB announced a breach of sensitive personal information. In U.S. litigation, the Third Circuit held that the number of visitors to an online privacy policy was relevant to whether the privacy policy was sufficiently user-friendly, the Fourth Circuit heard oral arguments regarding certification of various subclasses in a data breach case, and the Ninth Circuit upheld a TCPA defense win. At the international level, Vietnam implemented its long-awaited privacy law after issuing its first draft in 2021, and the European Parliament reached a deal formalizing a proposal to regulate artificial intelligence (AI), which, if passed, would be the worlds' first AI playbook.*

U.S. Laws and Regulation

CFPB Data Breach Raises Transparency and Security Concerns. On April 19, the Consumer Financial Protection Bureau (CFPB) publicly announced that a former employee sent confidential records to a personal email account, containing sensitive information about 45 financial institutions and approximately 250,000 customers. CFPB claimed it learned about the breach on February 14, but it did not inform lawmakers until March 21.

Washington Enacts Health Privacy Law. On April 27, Washington Governor Inslee signed the Washington My Health My Data Act (MHMDA) into law to protect health data not regulated by HIPAA. The law requires businesses to obtain consent (*i.e.*, opt-in) before collection and to provide consumers with rights, such as the right to opt out and the right to delete. Unlike other recent state laws, MHMDA contains a private right of action. Regulated entities must comply by March 31, 2024, and small businesses must comply by June 30, 2024. However, due to imprecise drafting, certain MHMDA requirements (*e.g.,* geofencing) could arguably to go into effect within months. For more information about the MHMDA, click here.

Indiana Enacts Comprehensive Privacy Law. On May 3, Indiana Governor Holcomb signed Senate Bill 5 (SB 5) — a comprehensive privacy law, similar to the existing Virginia Consumer Data Protection Act — into law. Like other state laws, Indiana's law will not apply to data subject to certain laws, such as the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, and Fair Credit Reporting Act, among others. Further, SB 5 applies only to consumer (and not employee) information. The law will take effect on January 1, 2026.

Montana and Tennessee Data Privacy Laws Await Governors' Signatures. On April 21, both the Montana (S.B. 384) and Tennessee (H.B. 1181) legislatures passed comprehensive privacy legislation, providing

consumers with rights to their data, such as the right to confirm processing, correct inaccurate personal information, and opt out of the sale of their personal information. If signed into law, Montana's law would take effect on October 1, 2024, and Tennessee's law would take effect on July 1, 2025.

U.S. Litigation and Enforcement

Court Holds Online Privacy Policy Traffic Is Relevant to Determine Policy Accessibility for Consent Purposes. On April 26, a federal judge granted in part and denied in part the plaintiff's motion to compel information, showing the number of people who visited Harriet Carter's online privacy policy. The case involved allegations that NaviStone, Inc., a marketing company hired by Harriet Carter, "intercepted" the plaintiff's communications on Harriet Carter's website, violating Pennsylvania's Wiretapping and Electronic Surveillance Control Act. One of NaviStone and Harriet Carter's defenses claimed that plaintiff impliedly consented to such interceptions because Harriet Carter's online privacy policy provided adequate notice of NaviStone's involvement. The plaintiff thus requested information about the number of visitors who found and opened the privacy policy, arguing its relevance as to whether the privacy policy was sufficiently user-friendly. According to the plaintiff, if the privacy policy only attracted minimal traffic, it would cast doubt on the defendants' claim that a reasonable person should have known about the privacy policy and its contents. However, NaviStone contended that the number of people who visited the privacy policy was irrelevant; the real question was whether the privacy policy existed and adequately disclosed its practices. The court disagreed, holding that the information was relevant but punted on whether its production would be unduly burdensome as NaviStone contended. Thus, the court ordered the plaintiff to take the deposition of NaviStone's corporate representative to determine whether production of the requested information would be overly burdensome.

Fourth Circuit Considers Class Certification in Marriott Data Breach. On May 3, the Fourth Circuit heard oral arguments, challenging the lower court's certification of various subclasses in a data breach MDL. Oral arguments focused on (1) Marriott's contractual class waiver argument; and (2) whether the district court's analysis of the plaintiffs' damages model, which formed the basis for their classwide calculation of damages, was sufficiently rigorous. Additional issues debated included whether the plaintiffs could proceed with a data breach case without demonstrating actual identity theft, and whether the size and complexity of the cases raised fundamental manageability issues.

The Ninth Circuit Upholds Defendant's TCPA Win. On April 13, in an unpublished opinion, the Ninth Circuit affirmed a district court's ruling in favor of a defendant health care company, holding the company did not violate the Telephone Consumer Protection Act (TCPA) by using an online text messaging service to send messages to consumers. In December 2021, a district court granted Concentra, Inc.'s motion for summary judgment with prejudice, reasoning that "because Textedly does not select the numbers to be messaged, change the sequence of the numbers that are entered into Textedly or determine the timing of the messages sent through its system," it is not an autodialer. The Ninth Circuit affirmed the district court's decision, emphasizing that Textedly did not store or produce randomly or sequentially generated telephone numbers.

Casino Employee Claims Careless Security Caused Data Breach. On April 17, an employee filed a class-action complaint against his casino and race track employer, alleging that the company failed to properly secure and safeguard its employees' personally identifiable information, including names and Social Security numbers. Specifically, the plaintiff claimed that the company stored their private information on a negligently and/or

recklessly configured database since files could be accessed without a password or multifactor authentication. The lawsuit followed a December 2022 data breach, which the company communicated to the affected individuals on April 10, after its investigation. The plaintiff contended the breach caused him and the proposed class members to face years of constant surveillance of their financial and personal records.

California AG Brief Supports Proposed California Age-Appropriate Design Code Act. On April 21, California Attorney General Rob Bonta opposed NetChoice LLC's motion for preliminary injunction, which requested to enjoin California from enacting the California Age Appropriate Design Code Act. NetChoice — a tech industry advocate whose members include Amazon, Google, Meta, TikTok, and Twitter — argued that the act would violate companies' rights under the First and Fourth Amendments, as well as other aspects of U.S. law. AG Bonta responded that the law does not regulate content or restrict expressive speech, and its "clear and specific requirements and prohibitions" ensure the protection of business rights. He also added that the act falls well within the state regulators' discretion to proactively protect children.

McDonalds Moves for Summary Judgment in AI Voiceprint Suit. On April 17, McDonalds filed a motion for summary judgment in a proposed class action, alleging that the fast food chain unlawfully collected consumers' "voiceprints" via artificial intelligence (AI) assistance at its drive-thru windows in violation of Illinois' Biometric Information Privacy Act (BIPA). McDonalds argued that the software merely recognized the content and not an individual speaker, and McDonalds took active steps to avoid collecting personally identifying data. Notably, BIPA does not define "voiceprint," but McDonalds argued the plain and ordinary meaning of "voiceprint" necessarily included the ability to identify an individual. In the earlier briefing, the court seemed to accept this definition.

Court Rules Insurers Must Pay Merck $1.4B for NotPetya Losses. On May 1, a New Jersey appellate court upheld the decision that insurers could not use the war exclusion in their insurance policies to deny pharmaceutical company Merck a payout after it suffered a cyberattack. After Merck downloaded accounting software infected with malware from Ukrainian firm NotPetya, over 40,000 machines in Merck's network became infected, causing major disruptions to sales, manufacturing, research, and development. The court held that no evidence sufficiently linked the attack to a Russian military action. This ruling exemplified a significant win for policyholders, seeking compensation for losses caused by cyberattacks through supply chain attacks, ransomware, and other malicious threats.

First Circuit Receptive to Reviving Rx Delivery Data Breach Suit. On May 2, the First Circuit heard oral arguments about reinstating a data breach lawsuit against home delivery pharmacy service company Injured Workers Pharmacy LLC (IWP). The proposed class of IWP's patients argued that a federal judge in Boston wrongly dismissed the suit, while also claiming the pharmacy failed to protect their private, personally identifiable information from a January 2021 cyber intrusion due to inadequate data security safeguards and employee training. The patients alleged they failed to receive any breach notification until almost nine months later, leaving their sensitive data vulnerable to cybercriminals. The proposed class sought relief from IWP for negligence, breach of contract, breach of fiduciary duty, unjust enrichment, and invasion of privacy. IWP responded that the risk of fraud from the cyber intrusion did not cause injury sufficient to grant Article III standing. The proposed class asked the court to certify the case as a class action, and requested relief to prevent IWP from further deceptive and unfair practices involving the breach.

International Regulation and Enforcement

Vietnam Publishes Personal Data Protection Decree. Vietnam's government published its Personal Data Protection Decree (PDPD), which implements principles around data collection, processing, and storage. The decree applies to all Vietnamese agencies, organizations, and individuals, as well as foreign agencies and organizations participating in or involved the processing of personal data in Vietnam. Like many comprehensive privacy laws, the PDPD requires organizations to provide privacy notices, conduct risk assessments, and implement appropriate security and safety measures. It further provides consumers with data subject rights, such as the right to be informed, the right to access, and the right to opt out, among others. Under the decree, organizations must notify the Ministry of Public Security within 72 hours of detecting a violation. The decree will take effect on July 1.

European Parliament Members Reach Political Deal on AI Rulebook. On April 27, the Members of European Parliament reportedly reached a deal to formalize a proposal to regulate AI based on its potential to cause harm. The legislation would contain certain prohibitions, such as the use of emotion-recognition, AI-powered software in the areas of law enforcement, border management, workplace, and education. If passed, it would be the worlds' first AI playbook.

Troutman Pepper Team Spotlight: Andrea Hoy

Andrea Hoy CISSP, CISM, MBA serves as a Troutman Pepper senior security advisor, supporting litigation and transactional attorneys on technical information security issues. She also cofounded and acts as CEO of Innovation Shipyard Alliance and as president and vCISO of A. Hoy & Associate. Previously, Andrea served as an advisor to the Pentagon, represented the U.S. as diplomat to China on eDiscovery and forensics, and advised the international board of directors for multiple cybersecurity companies. She also acted as an ISSA distinguished fellow in the cybersecurity profession and as an ISSA International president. Andrea received her MBA (*magna cum laude*) from Pepperdine University.

Upcoming Webinars, Podcasts, and Events

- Privacy + Security Forum Spring Academy, Washington, D.C., May 10-12
- NetDiligence Cyber Risk Summit, Philadelphia, May 31-June 2

Recent Troutman Pepper Publications

- Washington Legislature Goes Big With “My Health My Data Act”
- Washington Robocall Bill Signed Into Law
- Cookies and Online Tracking of Health Signals: An OCR Prescription for Potential Peril
- Florida Legislature Narrows Litigation-Spawning Telephone Solicitation Act
- DOJ Seizes Over $112 Million in Funds Linked to Cryptocurrency Investment Schemes
- The Ninth Circuit Reinforces Narrow Interpretation of ATDS under Borden Holding System Must Generate Random or Sequential Telephone Numbers to Constitute an ATDS

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