Articles + Publications | September/October 2023

More Privacy, Please – September/October 2023

WRITTEN BY

Molly S. DiRago | Ronald I. Raether Jr. | Kim Phan | James Koenig | Natasha E. Halloran | Robyn W. Lin

Editor's Note: The FTC continues to crack down on privacy and cybersecurity, including issuing a new warning to tax preparation companies and entering into a consent decree with 1Health.io. VPPA and BIPA litigation continues to dominate the courts, including a denial of a motion to dismiss regarding worker's voiceprints. In California, a federal judge enjoined enforcement of the Age-Appropriate Design Code Act. On the international level, Canada issued a Generative AI Code of Conduct for feedback, and the EU-DPF survives a court case.

U.S. Laws and Regulation

FTC Announces Consent Order With 1Health.io. On September 6, the Federal Trade Commission (FTC) entered into a consent order with 1Health.io alleging that 1Health.io failed to adequately protect DNA data and unfairly changed its privacy policy. 1Health.io, which offers DNA results for consumers, advertised to consumers that their DNA samples would be securely stored. The FTC alleged that the company put consumers' data at risk by storing unencrypted health, genetic, and other personal information in publicly accessible data buckets. The FTC also alleged that the company changed its privacy policy by retroactively expanding the types of third parties with which it could share consumers' data without notifying affected consumers or obtaining their consent.

FTC Warns Tax Preparation Companies on Tracking Technologies. On September 18, the FTC issued a warning to five tax preparation companies that the companies must obtain taxpayer consent prior to using any confidential information for unrelated purposes, such as advertising. The FTC also specifically warned that an unfair or deceptive practice includes the use of tracking technologies, such as pixels, cookies, APIs, or SDKs, to amass, analyze, infer, or transfer personal information in ways that a reasonable consumer would not expect, without first obtaining the consumer's express consent.

California Governor Orders State Agencies to Assess GenAI Risks. On September 6, California Governor Gavin Newsom issued Executive Order N-12-23, which directed state agencies to study the risks that generative artificial intelligence (GenAI) poses. Under the order, state agencies and departments must produce a report to explain how the state can benefit from GenAI, but also to assess the risks GenAI presents to individuals, communities, government and state government workers, and energy infrastructure. Specifically, the report must include, but is not limited to, "the risks stemming from bad actors and insufficiently guarded governmental systems, unintended or emergent effects, and potential risks toward democratic and legal processes, public health and safety, and the economy." Further, by March 2024, the California Cybersecurity Integration Center and the California State Threat Assessment Center must perform a joint risk analysis of potential threats to, and vulnerabilities of, California's energy infrastructure by the use of GenAI. The order included additional directives such as guidelines for public sector procurement and use of GenAI, trainings, and pilot projects.

54 AGs Call on Congress to Protect Children From AI. Attorneys general (AGs) from all 50 states and four U.S. territories sent a letter calling on Congress to evaluate and enact legislation preventing the use of artificial intelligence (AI) to exploit children through pornography. The effort urges lawmakers to establish a commission to study how to deter the use of AI to make child pornography, and expand the restrictions on child sexual abuse material. The AGs agree that AI is advantageous to society, but bad actors can utilize it to produce "deepfakes" using real photos and voice recordings to generate AI content showing children in sexual positions. This letter comes after a Senate subcommittee brought in OpenAI's CEO in May to testify on this technology. In June, U.S. senators also introduced legislation barring AI companies from claiming a broad liability shield.

Governor Newsom Signs the Delete Act Into Law. On October 10, California Governor Gavin Newsom signed the Delete Act into law. The Delete Act (SB 362) amends California's current data broker law to introduce additional disclosure and registration requirements on data brokers, and to require them to support deletion requests through a to-be-announced "deletion mechanism" developed and administered by the California Privacy Protection Agency (CPPA).

US Senator Seeks Clarity After 23andMe Dark Web Data Leak. After data from approximately five million users was allegedly leaked for sale on the dark web in batches over recent weeks, Louisiana Senator Bill Cassidy began probing into the genetic testing biotech company, 23andMe. Cassidy is the top Republican on the Senate's Health, Education, Labor, and Pensions Committee, and called on 23andMe's CEO to provide the committee with details on how the personal information collected from the company allegedly ended up for sale on the dark web. However, the company has denied this and said that it had not been breached.

Federal Agencies Behind on Implementing NIST Privacy Standards. Reports have shown that U.S. federal agencies like the Department of Justice and the Department of Housing and Urban Development are nearly five years behind in adopting the 2018 privacy recommendations from the U.S. National Institute of Standards and Technology (NIST). NIST previously advised federal agencies on integrating its risk management framework and privacy tools into the management practices of the federal agencies. However, after years since the NIST advisory, reports show full or even partial adoption has not come to fruition. The lack of implementation has many privacy experts concerned that the federal government is ill-prepared to handle a growing body of data, even as it seeks to embrace technologies like AI.

Twitter's 2018 Data Breach at Center of SEC Investigation. The SEC is probing X, formerly Twitter, over insufficient disclosures related to the company's 2018 data breach. The SEC has been critical in scrutinizing whether the former top executives, Ned Segal and Parag Agrawal, failed to adequately disclose privacy issues to shareholders or put in place proper controls to prevent further breaches. Twitter suffered several security breaches in 2018, including a bug that allowed outsiders access to user email addresses during password resets, revealing the identity of users. Another virus left passwords exposed and a security flaw in Twitter's system made it possible to identify the country codes of Twitter users' phone numbers, allowing outsiders to see where the accounts were based. In 2022, Twitter paid $150 million to settle FTC allegations over user data breaches. In Europe, Ireland's Data Protection Commission fined Twitter €450,000 over its breach in December 2020.

Governor Newsom Signs Reproductive Health and Immigration CCPA Amendments. On October 8, Newsom signed amendments to the California Consumer Privacy Act (CCPA) into law. The amendments contain a reproductive health data exemption, as well as the inclusion of immigration data when referring to "sensitive

personal data." When speaking about the reproductive health data exemption, Newsom stated that broad interpretation of the exemption could create unintended consequences within the existing CCPA exemptions. Newsom expressed the need for a "clean-up policy to ensure an appropriate balance."

NY DFS Amends Cybersecurity Regulations. New York Governor Kathy Hochul announced on November 1 that the state's Department of Financial Services (NY DFS) has amended its Cybersecurity Regulations to "enhance cyber governance, mitigate risks, and protect New York businesses and consumers from cyber threats."

According to the NY DFS, key changes in the regulations include:

- Enhanced governance requirements;
- Additional controls to prevent unauthorized access to information systems and mitigate the spread of an attack;
- Requirements for more regular risk assessments, as well as a more robust incident response plans;
- Updated notification requirements; and
- Updated direction for companies to invest in at least annual training and cybersecurity awareness programs that are relevant to their business model.

These newly amended compliance requirements will take effect in phases and continue to apply to "covered entities," including, but not limited to, those operating under, or required to operate under, a license, registration, or similar authorization under the Banking Law, the Insurance Law, or the Financial Services Law.

FTC Amends Safeguards Rule to Require Reporting of Data Breaches. The FTC has announced a final rule amending the Standards for Safeguarding Customer Information (Safeguards Rule) under the Gramm-Leach-Bliley Act. The Safeguards Rule requires nonbanking financial institutions to develop, implement, and maintain a comprehensive information security program to keep their customers' information safe. The amendment will require financial institutions to notify the FTC no later than 30 days after discovery of a security breach involving the information of 500 or more consumers. The FTC will deem a financial institution to have knowledge of a notification event if such event is known to any person, other than the person committing the breach, who is the financial institution's employee, officer, or other agent. The amendment will go into effect 180 days after publication of the final rule in the Federal Register.

U.S. Litigation and Enforcement

Sony Settles VPPA Class Action Suit for $16M. On September 16, Sony Pictures Entertainment, Inc. settled a putative class action suit for $16 million after the plaintiffs accused the company of gathering and sharing users' personal information through a tracking pixel without their consent in violation of the Video Privacy Protection Act (VPPA). Sony also agreed to modify the use of the third-party tracking technologies on portions of its streaming products relevant to VPPA compliance. According to the plaintiffs' unopposed motion for preliminary approval of class action settlement, this agreement is the largest VPPA-Pixel settlement to date. The court preliminary approved the settlement on September 28, and set the final approval hearing for December 19.

Judge Blocks California's Online Child Safety Law. On September 18, a federal judge enjoined the California Age-Appropriate Design Code Act (CAADCA), which imposes data privacy requirements on businesses that provide an online service, product, or feature likely to be accessed by a child. The court reasoned that the

CAADCA's commercial speech restrictions likely violate the U.S. Constitution's First Amendment. The court noted that while it is "keenly aware of the myriad harms that may befall children on the internet," it is "troubled by the CAADCA's clear targeting of certain speakers." The law requires platforms, before releasing any online products and services, to assess whether their offerings could harm children.

Casino Hit With Lawsuit After Cyberattack. On September 21, a plaintiff filed a proposed class action suit against MGM Resorts International (MGM) after the company suffered a 10-day cyberattack. The plaintiff asserts that on September 7, threat actors gained access to MGM's network by impersonating an IT admin. The threat actors then locked down MGM's network preventing resort guests from using their electronic room cards, Wi-Fi, ATM kiosks, electronic gaming devices, and other resort services. The complaint also alleges that MGM was aware of its vulnerability because its IT vendor prewarned the company and provided preventative tips to counter attacks against IT service desk personnel. Thus, the plaintiff seeks damages because the company's "'utter failure' to protect consumers' sensitive data presents risks to the data breach victims that 'will remain for their respective lifetimes.'"

College Reaches $3.5M Settlement With NY AG to Boost Its Data Security. On September 20, Marymount Manhattan College agreed to invest $3.5 million in data security enhancements. The settlement occurred in response to the Office of the AG of the State of New York's finding that the college's failure to maintain adequate safeguards made it vulnerable to a cyberattack in 2021 that exposed the personal data of 191,752 students, faculty, and alumni. Under the settlement terms, the college must, amongst other requirements, maintain a comprehensive information security program; comply with, and make public, its retention policy; and implement specific safeguards, including enabling multifactor authentication for users logging into its networks, maintaining a penetration-testing program, and appointing an employee responsible for the security program.

General Mills Succeeds on Tracking Pixel VPPA Class Action. A class action accusing General Mills of unlawfully sharing visitors' viewing behavior with social media companies has been scrapped by a California federal judge after finding the plaintiffs have not shown that General Mills is the type of business that falls under the VPPA. This comes after the federal judge similarly ruled against an earlier version of the case with leave to amend in June. Specifically, the judge held that plaintiffs failed to adequately plead that General Mills was a covered "video tape service provider", which is defined under the VPPA as one that is "engaged in the business … of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials."

Little Caesars Seeks $6.9M BIPA Settlement. Little Caesars is seeking preliminary approval of a $6.9 million settlement for a proposed class action on behalf of 8,407 workers, which alleges that Little Caesars violated Illinois' Biometric Information Privacy Act (BIPA) by not obtaining informed consent before scanning employees' fingers. In the settlement, Little Caesars has agreed that it "has or will delete, within 60 days of final settlement approval, all finger-scan data on the timekeeping system for its active and former employees," except for employees who have other pending lawsuits and data preservation orders.

Grocery Store Faces BIPA Voiceprint Suit. Former employees of Fresh Thyme Market have sued the grocery chain, pleading that the chain unlawfully collected, used, and stored the warehouse workers' voice print data by requiring them to use a Honeywell voice-identifying headset, and not providing them with the necessary disclosures or obtaining their express consent as required by BIPA. As a part of their onboarding, the former employees read a series of words to create a voice template that the device would then use and reference to

communicate with the employee while delegating work tasks. Judge Jenkins denied the defendant's motion to dismiss, stating it is reasonable to infer that the information Fresh Thyme had collected from its workers' Vocollect use is a "voiceprint" under Illinois' BIPA, despite it not having a clear definition. However, mere voice-recognition software alone is insufficient, said Judge Jenkins, through discovery, the former employees will have to show the data collected by the technology can identify someone.

International Regulation and Enforcement

Canada Publishes GenAI Code of Practice. The Government of Canada's Innovation, Science, and Economic Development is seeking comments and feedback on a GenAI Code of Practice. The code of practice follows six elements: Safety, Fairness and Equity, Transparency, Human Oversight and Monitoring, Validity and Robustness, and Accountability. The code would provide further guidance for developers, deployers, and operators of GenAI systems. This publication is the latest step that the Canadian federal government has taken to address privacy and cybersecurity.

EU-DPF Faces Litigation Challenges. The European Union (EU) General Court ruled against interim measures to pause implementation of the EU-U.S. Data Privacy Framework. French Member of European Parliament Philippe Latombe had filed against the transfer agreement and subsequent adequacy decision. The court held that Latombe could not prove the individual or collective harm the agreement raises.

Troutman Pepper Team Spotlight: Prestigious "Innovative Lawyers" Recognition

We are thrilled to share that our global Privacy + Cyber practice has been shortlisted for recognition in the prestigious 2023 Financial Times Innovative Lawyers Awards North America, in the category of Innovative Lawyers in Cyber Security & Data Protection. The annual awards, now in their 13th year, showcase the top law firms and in?house legal teams driving innovation in the North American legal sector.

Our entire practice and group co-leaders, Jim Koenig and Ron Raether, were nominated for this national recognition thanks in part to the team's 360-degree approach to privacy. This unique methodology leverages an integrated team of attorneys and professional staff, including former chief privacy officers, chief security officers, auditors, and industry executives. It allows us to extend the range of privacy and cyber services traditionally offered by law firms, drawing on our unique combination of global expertise in key areas such as privacy program creation and implementation, licensing, financing and M&A transactions, incident response, litigation, and regulatory investigations and enforcement.

The Innovative Lawyers North America 2023 rankings report is developed by the *Financial Times* in partnership with RSGI, a global think tank for the legal industry that focuses on growth and innovation for law firms. Winners are selected following a nomination cycle and extensive research that includes telephone interviews, questionnaires, and reviews. Market experts also assess the submissions and the research. Winners will be announced at the Innovative Lawyers Awards North America December 4 event at Gotham Hall in New York.

Past Webinars, Podcasts, and Events

- 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.

- Sadia Mirza (Conference Co-Chair), Net Diligence Cyber Risk Summit, October 16-18, 2023.

Recent Troutman Pepper Publications

- CFPB Outline Rulemaking Plan to Dramatically Alter Decades of FCRA Requirements for Everyone in the Consumer Data Ecosystem
- 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.

Safvet Besen is an associate with Troutman Pepper who is not licensed to practice law in any jurisdiction; application pending for admission to the California Bar.

RELATED INDUSTRIES + PRACTICES

- Artificial Intelligence
- Privacy + Cyber
- eDiscovery + Data Management