Articles + Publications | June 2023

More Privacy, Please – June 2023

WRITTEN BY

Molly S. DiRago | Natasha E. Halloran | Ronald Raether, Jr. | James Koenig | Kim Phan | Katie Rose Hancin | Robyn W. Lin

Editor's Note: *Montana became the latest state to pass a comprehensive privacy bill, joining California, Virginia, Colorado, Connecticut, Utah, and Tennessee. Florida, too, passed a privacy bill, but with a much narrower scope. Meanwhile, at the federal level, the House Energy and Commerce Committee continued to work on the federal analog: the American Data Privacy and Protection Act. In U.S. litigation, courts continued to see litigation under the Video Privacy Protection Act, including a new suit against Hearst Television. At the international level, European Parliament members adopted a nonbinding opinion to vote against the EU-U.S. Transfer Agreement, and the French CNIL leveraged a fine against Clearview AI for noncompliance.*

U.S. Laws and Regulation

Montana Passes Comprehensive Privacy Law. On May 19, Montana passed the Consumer Data Privacy Act (CDPA), joining the growing number of states that have passed comprehensive privacy laws. The law becomes effective October 24, 2024. The CDPA will apply to businesses in Montana that either (1) control or process personal data of at least 50,000 state residents; or (2) derive over 25% of gross revenue from the sale of personal data and control or process personal data of 25,000 or more state residents. It will create consumer privacy rights, such as access, correction, deletion, and portability. Like most other comprehensive state privacy laws, with the exception of California, the CDPA will include entity-level exemptions (*e.g.,* for financial institution regulated by the Gramm-Leach-Bliley Act).

US House Energy and Commerce Committee Begins Consideration of Federal Data Privacy and Security Law. The U.S. House Energy and Commerce Committee will begin updating the American Data Privacy and Protection Act (ADPPA) for re-introduction. The ADPPA passed the committee with a bipartisan vote on December 30, 2022. The committee's latest hearing highlighted ADPPA's strong protections for children under 17 by, for example, minimizing data collection on children; making it illegal to target advertising to children under 17; and treating all data on children under 17 as sensitive. The committee already held six data privacy hearings on the ADPPA just this year.

FTC Issues Warning on Biometric Information. On May 18, the Federal Trade Commission (FTC) issued a policy statement, expressing its concerns over the increased use of biometric information-related technologies. The FTC emphasized its commitment to combatting unfair and deceptive collection and use of biometric information and warned that making "false or unsubstantiated claims about the accuracy or efficacy of biometric information technologies or about the collection and use of biometric information" violates the FTC Act. In determining whether a business' collection or use of biometric information violates the FTC Act, the FTC will consider whether the business (1) properly assessed foreseeable harms to consumers; (2) promptly addressed

known or foreseeable risks; and (3) provided appropriate training for employees and contractors.

Florida Lawmakers Pass Privacy Bill Limiting Companies' Ability to Leverage Consumer Data. On June 6, Governor Ron DeSantis signed a new privacy bill that granted limited control over data usage to state residents, enabling consumers to discover what information companies collected about them and to request the deletion of certain data. However, these provisions would only apply to companies that either: (1) eclipse $1 billion in revenue; (2) derive at least half of their global revenue from ad sales; (3) operate a "smart speaker," with an integrated voice command component; or (4) run an app store with a minimum of 250,000 apps. The bill also would introduce requirements applicable to any online service, product, or features primarily accessed by a child. The protections offered to children are similar to those in California's Age-Appropriate Design Code.

OCR Strikes $350K Settlement Over HIPAA Violation. The U.S. Department of Health and Human Services Office for Civil Rights (OCR) settled a case with health care software services provider MedEvolve, Inc., regarding potential violations of HIPAA's security notification rules. The settlement occurred in the wake of a data breach investigation where a server containing the protected health information of over 230,000 individuals was left accessible online. According to OCR, the server held patient names, telephone numbers, billing addresses, and in some cases, even patient Social Security numbers. MedEvolve settled for $350,000 and agreed to implement a corrective action plan that addresses the violations and enhances patient data security.

FTC Fines Education Technology Provider Edmodo for COPPA Violations. On May 22, the FTC announced it had entered an order against education technology provider Edmodo for collecting personal data from kids without obtaining their parents' consent and for using that data for advertising in violation of the Children's Online Privacy Protection Act (COPPA). The order prohibited Edmodo from conditioning a child's participation in an activity on the child's disclosure of more information than reasonably necessary to participate in the online activity; banned the company from using intermediaries in the parental consent process; forbade the company from using children's information for noneducational purposes, such as advertising or building user profiles; and required Edmodo to delete models or algorithms using personal information collected from children without verifiable parental consent or school authorization.

FTC Proposes Amendments to Health Breach Notification Rule. On May 18, the FTC requested comments on proposed changes to the Health Breach Notification Rule (HBNR), especially concerning the HBNR's applicability to health apps and similar technologies. The proposed amendment would require vendors of personal health records (PHR) and related entities not covered by HIPAA to notify individuals, the FTC, and others in the event of a breach of unsecured personally identifiable health data. Comments are due July 17.

Mass Hack Breaches Fortra-Hosted Systems. In January 2023, hackers breached Fortra's Go-Anywhere file-transfer software used by thousands of organizations to share data sets across the internet, disclosing the personal and health information of millions of people. Since the breach, NationsBenefits, Community Health Systems, U.S. Wellness, Brightline, the city of Toronto, and other groups reported data thefts. On April 17, Fortra released a blog post, outlining the results of its own investigation and confirmed the issue was isolated to the GoAnywhere software, and on May 4, the U.S. Department of Health's Data Breach Portal confirmed more than three million individuals had their health data stolen, making this the third largest health data-related breach of 2023.

U.S. Litigation and Enforcement

Amazon Prevails in Alexa Suit. On May 2, a Washington federal district judge rejected the plaintiff's efforts to amend a class action against Amazon regarding Alexa software's collection of voice data to generate targeted ads for customers. Rejected for "merely repeat[ing] the same arguments the court ha[d] already rejected," Judge Barbara Jacobs Rothstein stood by her initial finding that did not preclude Amazon from using voice data captured by Alexa software to inform advertising. Further, even if the court accepted the customers' definition, the plaintiffs would have consented to such use.

Hearst Faces Proposed Class-Action Lawsuit Over Alleged Personal Data Sharing. On May 5, Hearst Television, the owner of multiple television stations and apps, including WCVB and WMUR, was hit with a proposed federal class-action lawsuit, alleging that their apps "knowingly and intentionally" share users' personal information with Google's DoubleClick and another third-party interface to increase ad rates. The lawsuit, filed in Boston, claimed that Hearst shared email addresses, location data, and the specific videos watched by users with DoubleClick and Braze, violating the Video Privacy Protection Act (VPPA). The complaint alleged that this data sharing allowed Hearst to maximize revenue by disclosing personally identifiable information to Google, making their apps more attractive to advertisers.

Court Dismisses FTC Data Privacy Suit Against Kochava. On May 4, a federal judge ruled in favor of mobile app analytics provider Kochava in an FTC-initiated data privacy suit. The judge dismissed the FTC's suit, which accused Kochava of unlawfully selling geolocation data that could enable third parties to track mobile device users to sensitive locations, but it granted the FTC 30 days to amend. The court found that the FTC had not adequately supported its claim that Kochava's conduct violated the unfairness prong of Section 5 of the FTC Act, reasoning that "the FTC has not alleged that Kochava's practices create a 'significant risk' of concrete harm." The judge also rejected Kochava's preemptive lawsuit, which attempted to block the agency's enforcement action without leave to amend, stating that Kochava failed to identify any viable cause of action that supported its claim for injunctive relief.

Discord Users Experience Data Breach. Discord recently warned users that their personal information may have been compromised after a hacker gained unauthorized access to a third-party customer support agent's account. Users learned that their email addresses, customer service messages, and attachments sent to Discord may have been exposed. With affected number of users still unknown, Discord has since deactivated the compromised account and is working to improve its security practices.

Boston Globe Strikes $5M VPPA Class-Action Settlement. On May 25, a federal judge granted preliminary approval for a $5 million class-action settlement between Boston Globe Media Partners LLC and its subscribers who alleged that Boston Globe shared their personal information with Facebook through a tracking code on the newspaper's website without their consent. Specifically, the plaintiff claimed that the company disclosed his personally identifiable information and video-watching behavior to Facebook in violation of the VPPA. Boston Globe agreed to suspend operation of the Facebook tracking pixel on its website until the VPPA is amended, repealed, or invalidated, or the company receives VPPA-compliant consent for the disclosure to Facebook. If approved at the September 7 hearing, the settlement would award give $4 million to subscribers and $1 million of in-kind relief for one-week extensions to existing digital subscriptions.

Eleventh Circuit to Re-Consider Standing in TCPA Class Actions. On June 13, the full Eleventh Circuit will hear arguments on the question of whether receiving a single unsolicited text message constitutes a concrete injury that establishes standing under the Telephone Consumer Protection Act (TCPA). In the 2019 *Salcedo v. Hanna* case, the Eleventh Circuit held that receipt of a single unsolicited text message does not establish standing for a TCPA claim. The *en banc* circuit will now decide whether to affirm this high bar for standing in TCPA class actions in light of the 2021 U.S. Supreme Court decision in *TransUnion v. Ramirez*, which held that plaintiffs must demonstrate concrete harm to obtain standing in federal courts. This challenge to standing under the TCPA arose from an August 2019 lawsuit against GoDaddy.com that accused the company of using an automatic telephone dialing system to send unwanted text messages. A now-vacated panel decision struck down the $35 million settlement due to concerns about whether all class members had standing to sue.

$4.3M Morley Data Breach Deal Receives Final Approval. On May 12, a Michigan federal judge granted final approval for a $4.3 million class-action settlement, with Morley Cos. agreeing to compensate nearly 700,000 individuals affected by an August 2021 ransomware attack. In early 2022, Morley notified current and former employees and clients that their personal information — including Social Security numbers, addresses, dates of birth, driver's license numbers, and health insurance information — may have been accessed by the cyber perpetrators. The plaintiffs filed the class action in February 2022 and reached a settlement in April 2022. In addition to compensating class members for the time and money they spent securing their personal information, Morley agreed to offer three years of credit monitoring and one year of password management services for all claimants. Morley also submitted documentation of the steps it took to enhance its data security.

UMass Hospital Agrees to Settle Kronos Data Breach Claims. On May 12, the University of Massachusetts Memorial Medical Center (UMass Memorial) agreed to pay $1.2 million to settle a data breach class-action and federal wage lawsuit. UMass Memorial workers brought the suit after a 2021 cyber breach of the workforce management company Kronos, Inc. rendered the hospital's payroll processing system unusable for more than a month. If approved, the settlement would compensate around 3,178 workers who were shorted pay due to the hack. The workers also intend to file an amended complaint to clarify their claims against lawsuit co-defendants Kronos and UKG, Inc.

International Regulation and Enforcement

MEPs Vote Against EU-US Framework. On May 11, members of the European Parliament voted to adopt a nonbinding opinion, rejecting the EU-U.S. Data Privacy Framework. The MEP highlighted concerns over U.S. foreign intelligence agencies' bulk data collection practices and the lack of a "lawsuit-proof regime." Rapporteur Juan Fernando López Aguilar said while the proposed EU-U.S. Data Privacy Framework provided a "significant improvement," it lacked elements regarding "judicial independence, transparency, access to justice, and remedies" to protect EU citizens' and businesses' data.

France Data Protection Authority Fines Clearview AI €5,200,000 for Delayed Compliance. On May 10, the French Data Protection Authority, Commission Nationale de l'Informatique et des Libertés (CNIL) announced that it fined Clearview AI €5,200,000 for failing to comply with an October 2022 order, which prohibited Clearview AI from collecting and processing the data of individuals living in France, and failing to delete the data of these individuals. The CNIL found that in two months, Clearview AI did not provide any proof of compliance.

Troutman Pepper Team Spotlight: Drew Mann

Washington, D.C. Consumer Financial Services Partner Drew Mann brings significant and highly relevant experience in the health care antitrust space, both from his time at the Federal Trade Commission (FTC) and in private practice.

Throughout his practice, Drew has conducted antitrust due diligence reviews for clients contemplating acquisitions, mergers, divestitures, or joint ventures in various industries. He has managed responses to voluntary access letters, U.S. agency information requests, including Second Requests, coordinated parallel state attorneys general investigations and federal congressional inquiries, provided training and counseling on gun-jumping issues, and overseen integration planning activities. Drew also has extensive government investigations experience, which includes successfully defending clients in enforcement actions brought by the FTC and U.S. Department of Justice, Antitrust Division.

Lastly, Drew has experience in matters related to joint ventures and corporate counseling. He has prepared firewall guidelines and regularly advised on structure and information exchange issues for joint ventures in the health care and energy industries. He also has provided antitrust compliance training, conducted global antitrust/competition audits, and created competition compliance materials.

For spring break this year, Drew and his wife Kara took their four daughters on a life-changing humanitarian trip to Tanzania, Africa. They built a classroom, taught health classes, filled empty library shelves with books, provided mattresses to village elders, distributed water filters, and drilled a well for a remote village.

Upcoming Webinars, Podcasts, and Events

- 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
- Peter Wakiyama, Kim Phan, Laura Hamady, and Graham Dean (Speakers), "ChatGPT FOMO? How to Craft Effective Privacy Policies for AI," Troutman Pepper, July 20, 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

Recent Troutman Pepper Publications

- Stephen Piepgrass, Ron Raether, and Dave Gettings (Speakers), "AI: Impact and Use in Background Screening ," Troutman Pepper, June 7, 2023

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, Esther Kye, Brandon Liu, Jon McNeal, Katie Hancin, and Alyssa Gao, 2023 summer associates with Troutman Pepper who are not admitted to practice law in any jurisdiction, also contributed to this newsletter.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber