Articles + Publications | July 2023

More Privacy, Please – July 2023

WRITTEN BY

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

Editor's Note: *Texas, Oregon, and Delaware became the latest states to pass a comprehensive privacy bill, while the CPRA, Connecticut, and Colorado's privacy laws came into force. In the litigation world, the FTC filed an amended complaint against Kochava, and the HHS settled with a psychiatric center that disclosed patient information in an online review. This month, international efforts focused on AI, as European Parliament members approved the AI Act, and the Japanese privacy watchdog warned OpenAI about collecting sensitive user data.*

U.S. Laws and Regulation

Texas Enacts Comprehensive Privacy Law. On June 18, Texas Governor Greg Abbot signed HB 4, the Texas Data Privacy and Security Act (TDPSA). TDPSA applies to anyone conducting business in the state of Texas and to any products or services consumed by Texas residents. However, the TDPSA carved an exception for companies defined as "small businesses" by the U.S. Small Business Administration. Other entities exempted from the TDPSA include financial institutions, nonprofits, and higher education institutions. Certain data also exempted includes protected health information under the Health Insurance Portability and Accountability Act and data regulated under the Fair Credit Reporting Act. The TDPSA placed additional responsibility on data controllers, such as requiring opt-in consent to use sensitive personal information. Most of the provisions take effect on July 1, 2024, and the law takes full effect — including universal opt-out provisions — on January 1, 2025.

Oregon Nears Comprehensive Privacy Law. On June 26, the Oregon Legislature passed SB 619 to protect consumer personal data. Unlike other state privacy laws, the bill would require controllers to provide consumers with a list of specific third parties to whom their personal data had been disclosed. Additionally, the bill would only exempt information regulated by the Gramm-Leach-Bliley Act, but it would provide an exemption for insurers that meet the definition under Oregon law. The bill awaits signature from Governor Tina Kotek. If signed, the act will take effect July 1, 2024.

Delaware Passes Comprehensive Privacy Law. On June 30, the legislature passed the Delaware Personal Data Privacy Act — a bill similar to Connecticut's Data Privacy Act, with a few exemptions. Unlike other state laws, the bill would not provide an entity-level exemption for HIPAA-covered entities and business associates, and it would not exempt institutions of higher education. The bill would, however, apply to nonprofits. The bill awaits signature from Governor John Carney. If signed, the bill will take effect January 1, 2025.

Connecticut Data Privacy Act Comes Into Force. On June 5, Attorney General Tong reminded businesses and consumers that the Connecticut Data and Privacy Act (CTDPA) would go into effect on July 1. The CTDPA applies to businesses that either conduct business in Connecticut or offer products or services targeted to Connecticut residents. Additionally, during the prior calendar year, these individuals or businesses must have controlled or

processed the personal data of either at least 100,000 consumers, or at least 25,000 consumers, while deriving over 25% of their gross revenue from the sale of personal data. CTDPA also applies to service providers, or "processors," that maintain or provide services involving personal data on behalf of covered businesses. Under the CTDPA, businesses must limit their collection of personal data; be transparent about how they use and secure that data; and obtain consumer consent before collecting sensitive information, such as precise location data, biometric information, and certain kinds of health data. Connecticut residents also will receive certain data subject rights to access personal data, correct inaccuracies in their personal data, delete their personal data, and opt out of the sale of their personal data and targeted advertising.

Connecticut Online Privacy Bill Signed by Governor. On June 26, Connecticut Gov. ed Lamont signed Senate Bill 3 (SB 3) — "an act concerning online privacy, data and safety protections." The bill amends the CTDPA and goes into effect on July 1, along with the CTDPA. The bill most notably expands the CTDPA to include consumer health data defined as personal data that can identify a consumer's physical or mental health condition, including gender-affirming health data and reproductive or sexual health data. The bill also prohibits geofencing of certain health facilities, establishes additional requirements concerning minors' personal data and social media accounts, establishes a duty of care owed by online dating operators to users relating to potential criminal activity of other users, and requires employers to disclose known instances of sexual harassment and assault when making employment recommendations for former employees.

SEC Admits to Broader Database Breach Than Initially Told. On June 2, the U.S. Securities and Exchange Commission (SEC) announced that the scope of its enforcement teams' improper access to documents was broader than initially revealed. The SEC originally announced the breach on April 5, admitting to a control deficiency that allowed enforcement division staff to view a staff-drafted memoranda in their general counsel's office, which should have been restricted to commissioners and attorneys who advise on SEC decisions. The SEC previously stated that the improper exposure only impacted two cases. However, in its recent statement, the SEC revealed the improper access potentially affected nearly 90 pending cases. SEC Chair Gary Gensler stated that he started the remediation process, which includes enhancing access controls to prevent files from being uploaded to the wrong databases in the future.

Bipartisan Senators Support Bill Protecting US Personal Data. On June 14, a group of bipartisan U.S. senators reintroduced legislation known as the Protecting American's Data from Foreign Surveillance Act, which would block the export of sensitive information to countries deemed "high risk" by the U.S. Department of Commerce. Under the proposed bill, only the transfer of personal information to places the Commerce Department deems "unworthy" would be restricted, and transfers to those places would only occur if companies could prove they had a "valid reason." Transfers to countries with enough privacy safeguards to prevent sensitive data from further transfers would be deemed "trustworthy" and would not be regulated. Calls to implement such legislation came after TikTok became the subject of critique, and reports indicated the app could track user keystrokes and access U.S. users' personal data.

OMB Extends Software Self-Attestation Deadline. On June 13, the Office of Management and Budget (OMB) released an update to a September 2022 memorandum (M-22-18) that focused on enhancing the security of the software supply chain through secure software development practices. The memorandum reaffirmed the importance of secure software development practices, but extended the deadline for agencies to collect self-attestation forms from contractors. The updated guidance said the OMB will give agencies three months to collect

forms from critical software providers, and six months for all software vendors on their networks after approving a common attestation form. This update gave software providers and federal agencies more time to follow the security requirements effectively. It is unclear when the common attestation form will be finalized, but a draft based on the National Institute of Security and Technology's Secure Software Development Framework exists.

MOVEit Bug Affects US Department of Energy. On June 15, the Department of Energy (DOE) announced that the global ransomware cyberattack on Progress Software Corp.'s file transfer tool MOVEit compromised DOE records as a result of a security bug. Government officials previously warned that a notorious Russian-speaking ransomware gang called "CL0P" was exploiting MOVEit's security bug. The DOE received ransom requests from CL0P at its nuclear waste and scientific facilities. However, CL0P themselves stated that "WE DON'T HAVE ANY GOVERNMENT DATA," and suggested that if they did acquire such data, they would "STILL DO THE POLITE THING AND DELETE ALL." In response to the 2023 attack, the DOE took preventative steps to stop future attacks on the MOVEit vulnerability, including notifying CISA, law enforcement, and Congress about the breach and the department's mitigating measures. If you are a MOVEit Transfer customer, you can find mitigation instructions here.

FTC Requests Public Comments on Health Breach Notification Rule Proposed Amendment. On June 9, the Federal Trade Commission (FTC) announced a notice of proposed rulemaking and request for public comment on an amendment to the Health Breach Notification Rule (HBN Rule). The rule applies to vendors of personal health records and related entities not subject to HIPPA, requiring them to notify individuals, the FTC, and as applicable, the media about breaches of private health data. Proposed changes to the HBN Rule would revise certain definitions, clarify the rule's scope, enhance notification requirements, and enhance overall clarity. The agency will accept written comments until August 8.

DHS Issues Final Rule to Add Additional Privacy Measures for Controlled Unclassified Information. On June 21, the U.S. Department of Homeland Security (DHS) issued a final rule, which implements further security and privacy measures for controlled unclassified information (CUI) into the Homeland Security Acquisition Regulation (HSAR). In support of the final rule, DHS cited high-profile breaches of federal information, highlighting the need for effective information security protections. The final rule identifies proper CUI handling requirements, improves incident reporting requirements, requires sanitization of government information, and requires contractors to have procedures in place to notify individuals whose personal information was exposed during a data breach. The final rule will become effective July 21.

U.S. Litigation and Enforcement

Maryland Resident Alleges TCPA Violation by P&G. On June 1, a Maryland resident filed a class-action complaint against The Proctor & Gamble Co. (P&G), claiming the company violated both the federal Telephone Consumer Protection Act (TCPA) and the Maryland Consumer Protection Act. Specifically, the complaint alleged P&G continued to send the plaintiff unsolicited text message advertisements even after she informed the company that she did not want to receive the messages. The complaint proposed three classes, all affected by P&G's alleged messaging scheme and seeks damages and injunctions blocking P&G from sending future unsolicited message advertisements.

Class Action Claims Hawaii Credit Union Failed to Timely Notify Customers of Data Breach. On June 2, a

new class of plaintiffs brought suit against HawaiiUSA Federal Credit Union for negligence, breach of implied contract, intrusion upon seclusion, and violations of Hawaii business statutes. The complaint cited a December 2022 data breach that allegedly affected approximately 20,889 individuals. The complaint asserted that although HawaiiUSA knew of the breach in March, it failed to notify customers until April 5, and as a result of the breach, customers will remain "at a heightened and unreasonable risk of identity theft for the remainder of their lives."

Court Sentences Former Air Force Lieutenant Colonel to Three Years for Mishandling Classified Documents. On June 2, a Florida federal court sentenced former Air Force Lieutenant Colonel Robert Birchum, who served for 29 years, to three years in prison, three years of supervised release, and a $25,000 fine. In 2017, law enforcement officers discovered that Birchum removed more than 300 classified files from authorized locations and kept them in his home, his overseas officer's quarters, and a storage pod in his driveway. The U.S. attorney asserted that Birchum knew he violated multiple nondisclosure agreements and disregarded many trainings on how to handle classified information, and his conduct "posed great risk to our national security." In sentencing, the court ignored Birchum's pleas to keep his incarceration under 60 days to preserve his Veterans Administration benefits.

FTC Amends Complaint Against Kochava. On June 5, the FTC filed an amended complaint against mobile data broker Kochava for allegedly selling sensitive geolocation data. The agency's particular concern involved the data's potential to reveal travel to abortion clinics, thereby exposing individuals who seek abortions or medical providers who perform the procedure. Company officials said the data could easily be obtained through other, legal means, and the conclusions drawn about people's objectives at certain locations require some unreliable inferential leaps. For now, the amended complaint remains sealed due to trade secret and confidentiality concerns.

New Jersey Psychiatry Practice Settles for Allegedly Posting Patient Health Information Online. On June 5, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced a $30,000 settlement, resolving a complaint against Manasa Health Center LLC. The health care provider, which provides adult and child psychiatric services in New Jersey, disclosed the private health information of four patients after those patients posted negative online reviews about the center. Specifically, the Manasa Health Center revealed details of patients' individual diagnoses and mental health treatments via public responses to the patients' negative reviews. In addition to the $30,000 paid to OCR, the center must begin a corrective action plan to ensure compliance with the Health Insurance Portability and Accountability Act Privacy Rule. OCR will monitor the center's progress for two years.

Fired Executive Proclaims 'Profits Over Privacy.' A June 14 lawsuit filed by former Grindr Privacy Chief Officer Ronald de Jesus accused company executives of ignoring warnings about user data and repeatedly violating state and international privacy laws by collecting and retaining highly sensitive information, including nude photos, without user consent. These allegations were raised in a wrongful termination and retaliation lawsuit filed by the former executive who claimed that he was let go after he identified a technical bug that allowed user data to be stored, even after an account had been deleted. De Jesus further contended that other firm executives brushed off his concerns, and hours after he sent a strongly worded email about potential illegalities, the company fired him. In response to these allegations, a company spokesman said these claims were "inaccurate," and De Jesus was terminated due to his "ineffective management of Grindr's privacy practices that put Grindr and its users at risk."

Eleventh Circuit Keeps Workers' Class Action Alive. On June 9, the Eleventh Circuit revived a proposed class-action lawsuit brought by warehousing company employees whose data was leaked in a 2020 ransomware attack, allegedly exposing the personal information of about 140,000 people. Workers argued that Americold Realty Trust erroneously won dismissal of the case despite failing to address a new foreseeability standard announced under a similar cyberattack case in *Ramirez v. The Paradies Shops LLC*. The appellate panel agreed with the workers that the recent *Ramirez* decision "undermined" the district court's dismissal of the claims against Americold and remanded the case to allow the plaintiffs leave to amend.

PetSmart Settles for $425K Ending Class-Action Biometric Data Lawsuit. PetSmart approved a $424,555 settlement agreement on June 8 to end a class-action lawsuit over accusations that the company improperly collected biometric voice data from workers in an Ottawa, IL warehouse. The plaintiffs initially sued PetSmart, alleging the company violated the Illinois Biometric Information Privacy Act by using a Vocollect order picking system. Specifically, Stegmann and the class members claimed that PetSmart failed to (1) notify their employees that their biometric information was being collected; (2) properly inform their employees of how long their biometric information would be maintained; (3) provide a retention schedule for the biometric information; and (4) obtain a written release to collect their employees' biometric information. The settlement agreement provided $899.27 in compensation to each of the 472 class members, permitting them to choose either a check payment or paid time off. The settlement agreement terms and proposed preliminary approval order awaits approval by U.S. District Judge Thomas Durkin.

International Regulation and Enforcement

Japan's Privacy Watchdog Warns ChatGPT-Maker OpenAI on User Data. Japan's privacy watchdog organization Personal Information Protection Commission (PIPC) recently warned OpenAI — the startup that developed the ChatGPT chatbot — about the dangers of collecting sensitive personal data without obtaining explicit consent. PIPC emphasized the need to balance privacy issues with the potential benefits of generative AI, while in contrast, the EU created a taskforce to establish rules to govern AI. OpenAI CEO Sam Altman suggested in May that the company might leave the EU if it's too difficult to comply with the AI regulations. Altman also met with Japanese Prime Minister Fumio Kishida in April to discuss AI regulation and the possibility of OpenAI expansion to Japan.

EU Approves AI Act. The European Parliament approved the EU AI Act, which intends to protect consumers from potentially dangerous applications of artificial intelligence. In next steps, the EU AI Act will undergo negotiations with the European Council. The EU AI Act introduces restrictions to address concerns over potential negative uses of AI, including surveillance and misinformation. The legislation requires firms to publish data use summaries to train their tools and establishes a risk system, whereby use of AI would fall under a risk level (unacceptable, high, limited, and minimal or no risk). The obligations imposed on businesses and users would thus depend on the level of risk.

Troutman Pepper Team Spotlight: Tim. St. George

Richmond Partner Tim St. George defends institutions nationwide facing class actions and individual lawsuits, while focusing his practice on complex litigation and business disputes, financial services litigation, and consumer litigation in federal and state courts at both the trial and appellate levels.

Tim brings particular experience in litigating consumer class actions, including industry-leading expertise in cases arising under the Fair Credit Reporting Act and its state law counterparts. He currently teaches the basic and advanced FCRA certification courses for the Professional Background Screening Association, the leading trade association for background screening companies and employers conducting screening. Tim also serves as outside general counsel for several background screening companies.

In his free time, Tim enjoys running around a soccer field (frequently losing the ball) and chasing around his three boys under six years old.

Upcoming Webinars, Podcasts, and Events

- James Koenig, Peter Wakiyama, and Kim Phan (Speakers), "Navigating the AI Landscape: Privacy, IP, Policies and More – An Industry Expert Roundtable," Troutman Pepper, July 20, 2023
- Troutman Pepper and Innovation Shipyard Alliance (Hosts), CISO/CSO/General Counsel Summit, September 15, 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
- 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

Recent Troutman Pepper Publications

- Storm Clouds Form Offshore Under the Updated Florida Electronic Health Records Exchange Act

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.

Lisa Amador, Phoebe Cooper, Julia Crooks, Patrick DeSabato, Ben Duwve, Esther Kye, Courtney Le, Emily Makar, Kaleem Shahzad, Justin Stalberg, Max Sun, Samantha Weber, Summer Xia, 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
- eDiscovery + Data Management