Articles + Publications | February 2021

More Privacy, Please – February 2021

WRITTEN BY

David N. Anthony | Ronald I. Raether Jr. | Ashley L. Taylor, Jr. | Angelo A. Stio III | Wynter L. Deagle | Yarazel Mejorado | Anne-Marie Dao | Sharon R. Klein

Do you want a simple way to keep current on important privacy changes? Avoid sleepless nights wondering whether you missed a privacy speed bump or pothole between annual updates? Worry no longer. Troutman Pepper is pleased to offer *More Privacy, Please* — a monthly newsletter recapping significant industry and legal developments, as well as trends in the areas of cybersecurity, information governance, and privacy.

U.S. LAWS AND REGULATION

- **2021 Washington Privacy Act Under Review in Senate Committee.** Washington's state legislature is again considering consumer data privacy legislation, after previous versions of the bill failed in 2019 and 2020. This year's Washington Privacy Act (WPA) continues to address the private sector's processing of personal data, while introducing regulations concerning the processing of personal data for public health emergencies (*e.g.,* contact tracing). The proposed law will govern entities conducting business in Washington or producing products or services targeted to Washington residents with certain user and revenue thresholds. The WPA includes provisions similar to those in the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), including a requirement for data controllers to enter into written agreements restricting their processors' control of data. If passed, the WPA would take effect on July 31, 2022.

- **New York State Lawmakers Re-Introduce Biometric Privacy Law.** On January 6, a bipartisan group of New York lawmakers introduced the Biometric Privacy Act, which, if passed, will limit private sector collection or disclosure of biometric identifiers and biometric information. The law also will impose notice and consent requirements, require security measures for biometric data storage, and allow for private rights of action for violations. If passed, New York will join the short, but growing list of U.S. states (Texas, Washington, and Illinois) passing biometric privacy legislation. Businesses using biometric data should closely monitor this bill's progress since — as Illinois Biometric Information Protection Act (BIPA) litigation has demonstrated — the proposed law's private right of action could mean costly litigation.

- **Virginia, Oklahoma, and Minnesota Consider Consumer Data Privacy Legislation.** In Virginia, Senate Bill 1392 was introduced on January 13 and largely mirrors the 2021 WPA discussed above. If passed, the law will go into effect on January 1, 2023. In Oklahoma, House Bill 1130 was introduced on January 15 and will require businesses to post policies explaining their data collection and privacy practices, though it would not grant Oklahoma residents any rights over their personal information. If passed, the law will go into effect on November 1, 2021. Finally, in Minnesota, HF 36 was introduced on January 7 and will require businesses to provide consumers rights over their personal information, including the right to access, opt out and request deletion. If passed, the law will go into effect on June 30, 2022.

- **Annual Updates to Privacy Policies for CCPA-Regulated Businesses are Due.** As a reminder, the CCPA requires covered businesses to update their privacy policies annually. For those organizations that issued privacy policies so that this anniversary coincides with the CCPA's January 1, 2020 effective date, an updated privacy policy is now due. Updating your privacy policy at least annually is a good practice to assure that any changes in information practices align with these consumer facing statements.

U.S. LITIGATION AND ENFORCEMENT

- **Marriott Beats Data Breach Litigation Due to Plaintiff's Failure to Plead Required Injury-in-Fact.** In *Rahman v. Marriott International, Inc.*, the U.S. District Court for the Central District of California dismissed data breach claims against Marriot for lack of subject matter jurisdiction, finding that the data compromised was not sensitive information as required by the Ninth Circuit to establish injury-in-fact for Article III purposes. The complaint alleged that class members were victims of a cybersecurity breach when two members of a Marriott franchise in Russia accessed class members' names, addresses, phone numbers, email addresses, genders, birth dates, and loyalty account numbers without authorization. Marriott confirmed that while names, addresses, and other publicly available information were obtained in the breach, no sensitive information (such as social security numbers, passport numbers, or credit card information) was accessed. In dismissing the complaint, the court reaffirmed that absent disclosure of sensitive information, there was no credible risk of identity theft risking real, immediate injury. As a result, the plaintiff had not suffered an injury-in-fact and could not meet the constitutional requirements of standing.

- **Excellus to Pay Over $5M to Settle Potential HIPAA Violations.** On January 15, the U.S. Department of Health & Human Services (HHS) announced that Lifetime Healthcare Companies, which includes Excellus Health Plan, Inc., agreed to pay $5.1 million to the Office for Civil Rights and to implement a corrective action plan to settle potential HIPAA violations. The Resolution Agreement and Corrective Action Plan detail Excellus' corrective action obligations, including implementing a security management process (which includes developing a risk management plan to address and mitigate security risks), developing policies and procedures for HHS approval, and reporting Excellus policies and procedures compliance failures to HHS within 60 days. The Corrective Action Plan will be effective for a period of two years.

- **Flo Settles Health Data Disclosure Allegations with the FTC.** On January 13, the Federal Trade Commission (FTC) published a proposed settlement with Flo Health, Inc. resolving allegations that the company improperly shared users' health information with outside data analytics providers. The FTC alleged that the popular fertility-tracking app developer provided its users' private health data to marketing and analytics companies without notice and without limiting how those third parties could use the data. Once the consent order is finalized, Flo will be required to: (1) properly represent users' control over their data and the company's compliance with any privacy, security, or compliance program; (2) send its users a detailed notice about the types of personal data Flo shares with data analytics firms; and (3) instruct third parties that received health data to destroy that data.

- **Illinois BIPA Lawsuit Filed Against "Interactive Voice Response" Software Provider.** On January 26, a class action complaint was filed against Nuance Communications, Inc. in Illinois state court. The complaint alleges that Nuance's interactive voice recognition (IVR) software, used by companies, such as FedEx, "collects and analyzes callers' actual voiceprints to understand the caller's request and automatically responds with a personalized response instead of simply providing menus of options from which the caller can press a number to select what they wish to accomplish." This collection, according to the complaint, violates Illinois' BIPA. This suit has enormous implications for companies using IVR software. Most companies employing such software receive a high volume of calls and rely on IVR to efficiently route and resolve those calls. For example, the complaint alleges FedEx receives 500,000 calls each day. Because it is not feasible for such companies to provide a written policy and obtain written consent from each caller, if this conduct constitutes a BIPA violations, companies will have no choice but to cease using IVR software at least when Illinois residents call in. While the complaint only named Nuance (*e.g.,* not FedEx), companies using IVR may face exposure for such use in the future.

INTERNATIONAL REGULATION AND ENFORCEMENT

- **EDPB Issues Draft Guidelines on Data Brach Notification.** On January 18, the European Data Protection Board (EDPB) released draft Guidelines 01/2021 on Examples Regarding Data Breach Notification, intended to complement its initial guidelines on personal data breach notification under GDPR adopted by the Article 29 Working Party in February 2018. The new guidelines — which include examples of common data breach

scenarios — aim to assist data controllers handling data breaches, including identifying factors to analyze when conducting risk assessments determining remediation obligations and whether to report a breach to relevant supervisory authorities and/or the affected data subjects.

- **Italian Data Authority Orders TikTok to Ban Unverified Accounts.** On January 22, Italy's data protection authority (GPDP) ordered the video app TikTok to block the accounts of any users in Italy whose age it could not verify. The ban will last until at least February 15 and comes after the GDPD's recent criticisms of TikTok for its insufficient protection of minors, lack of transparency in data privacy disclosures, and the use of default settings not respectful of users' privacy.

- **European Privacy Regulators Focus on Employers' Collection of Workers' Data.** EU data protection authorities are increasingly focused on employers' collection of employees' personal data, as reported by *The Wall Street Journal*. In Germany, German electronics retailer notebooksbilliger.de was recently fined €10.4 million ($12.6 million) for using video surveillance cameras to monitor employees, while in October 2020, fashion retailer Hennes & Mauritz AB was fined €35.3 million ($41 million) for collecting employees' personal data, including data about their health and religion, and disclosing that information to managers at its service centers. Under the GDPR, companies using video surveillance must justify their use of that type of surveillance.

RECENT TROUTMAN PEPPER PUBLICATIONS

- No Federal Court Standing for Data Breach Claims Alleging Theft of Non-Sensitive Personal Information
- 7th Circuit Challenges Whether Plaintiffs Had Standing in Recent District Court Cases
- District Court Finds Calls to Cell Phones Do not Violate the TCPA's Prohibition Against Telephone Solicitations to Residential Telephone Subscribers
- Mass. Uber Ruling Offers Insights on Online Contracts
- Home Security Company Will Pay $600,000 Civil Penalty in FCRA Settlement for Failing to Provide Risk-Based Pricing Notice
- Game On! Biden Nominates Chopra to Lead the CFPB
- One Ring Too Many – FCC Caps Number of Exempt TCPA Calls
- 29 States File Amicus Brief Supporting FTC's Authority to Obtain Monetary Relief in the Supreme Court
- Online Retailer Settles with State Attorneys General Over Security Incident

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber