Articles + Publications | December 2020

More Privacy, Please – December 2020

WRITTEN BY

Ronald Raether, Jr. | David N. Anthony | Angelo A. Stio, III | Ashley L. Taylor, Jr. | Wynter L. Deagle | 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

- **California (Expanding CCPA):** On November 3, California voters passed Proposition 24 during the 2020 general election to adopt the California Privacy Rights Act of 2020 (CPRA). The CPRA amends the California Consumer Privacy Act of 2018 (CCPA) in several ways intended to enhance consumer privacy protections. The CPRA becomes effective on January 1, 2023, except for certain provisions that will take effect on January 1, 2021. In the interim, the CCPA will remain in full force and in effect. For a more detailed analysis of the CPRA, please read Troutman Pepper's recent article.

- **Massachusetts (Auto OEMs):** Massachusetts voters passed SD645 Question 1, which enacts SD645 and amends and broadens a landmark 2012 "right to repair" law requiring automakers to use a nonproprietary standard for its onboard diagnostics port — the physical port used by dealerships to retrieve data. The amendment, which passed by a 75% voter margin, will compel auto manufacturers selling vehicles with telematics systems in Massachusetts to equip them with a standardized open data platform beginning with model year 2022 (which may be sold as early as January 2021). The standardized open data platform must give vehicle owners and independent mechanics the ability to access and retrieve mechanical data from the telematics system and run diagnostic testing through a mobile-based application. On November 20, the Alliance for Automotive Innovation — a trade group representing General Motors Co. and other leading auto manufacturers — sued Massachusetts Attorney General Maura Healey in a bid to block the measure. The complaint alleges the amendment is unenforceable because it is preempted by several federal laws, including the Computer Fraud and Abuse Act and the National Traffic and Motor Vehicle Safety Act.

- **Michigan (Search and Seizure):** Michigan voters overwhelmingly approved a state constitutional amendment requiring law enforcement officers to obtain a search warrant to access a person's electronic data or electronic communications under the same conditions currently required by the government to obtain a search warrant to search a person's house or seize a person's belongings. This amendment removes any remaining ambiguity as to whether law enforcement officers must obtain a warrant before searching a criminal suspect's text messages, internet search history, online chatroom participation, etc.

U.S. LITIGATION AND ENFORCEMENT

- **Zoom Settlement with the FTC (Privacy Policy Promises):** On November 9, the Federal Trade Commission (FTC) announced a settlement with videoconferencing platform Zoom over "misleading claims" about its security. Among other violations, the FTC alleged that since at least 2016, Zoom misled users by claiming to offer "end-to-end, 256-bit encryption" to secure users' communications, when in fact Zoom maintained cryptographic keys that allowed Zoom to access the content of customers' meetings and secured its Zoom Meetings in part with a lower level of encryption. In addition to the end-to-end encryption issue, the FTC also said that Zoom had stored unencrypted meeting recordings on its servers for up to 60 days and compromised the security of some users when it "secretly" installed software called ZoomOpener last year. As part of the settlement, Zoom must take specific measures to address the problems identified in the complaint, including (1) establishing and implementing a comprehensive security program, (2) refraining from making privacy and security misrepresentations, (3) reviewing software updates for security flaws to ensure the updates will not hamper third-party security features, (4) undergoing an independent audit of its security program every two years, and (5) informing the FTC of any data breaches.

- **BIPA Lawsuit Proceeds Against Apple (Required Injury for Standing to Sue):** On November 12, Chief Judge Nancy J. Rosenstengel of the U.S. District Court for the Southern District of Illinois rejected Apple, Inc.'s efforts to dismiss a class action alleging its facial recognition software violates Illinois' Biometric Information Privacy Act (BIPA) by collecting facial geometries from user pictures stored in the photo app on Apple devices. Judge Rosenstengel allowed the allegation that Apple violated BIPA by collecting the biometric information to proceed in federal court, concluding that the plaintiffs have standing because they allege Apple never received informed consent before collecting facial scans within the photos app. Judge Rosenstengel agreed with Apple, however, that the federal court lacked subject matter jurisdiction over the following two allegations because the plaintiffs failed to allege that they suffered a particularized injury-in-fact as opposed to alleging Apple's software posed a threat of generalized injury to the public: (1) the allegation that Apple possesses the biometric information without having created a retention policy as to when it would destroy the information, and (2) the allegation that Apple is profiting by selling devices with the facial recognition software.

INTERNATIONAL

- **Canada (Expanding Privacy and Enforcement):** Canada's minister of innovation, science, and industry introduced a new bill in the Canadian House of Commons on November 17 to create significant privacy reforms. The bill — titled the Digital Charter Implementation Act, 2020 — includes various measures to comply with Canada's Digital Charter, such as requiring plain language to obtain consent, giving increased personal control over digital information, and enforcing stricter fines. It also establishes the Personal Information and Data Protection Tribunal, which will levy administrative monetary penalties and hear appeals of orders issued by the Office of the Privacy Commissioner. If passed, the bill will enact the Consumer Privacy Protection Act and the Personal Information and Data Tribunal Act.

- **European Health Data Space:** On November 17, the European Data Protection Supervisor (EDPS) issued a preliminary opinion on the European Commission's strategy for data and framework to create a European Health Data Space (EHDS). The opinion states that EDPS supports a health data exchange but "underlines the necessity for data protection safeguards to be defined at the outset of the creation of the EHDS." Additionally, the EDPS called for the EHDS to come with a "robust legal basis" and work to narrow the fragmentation of current rules for health data processing.

- **Post-Schrems II Data Transfers:** On November 10, the European Data Protection Board issued two sets of recommendations that collectively outline a methodology for conducting international data transfers under the EU General Data Protection Regulation. The guidance consists of new "recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" and updated "recommendations on the European Essential Guarantees for surveillance measures." This guidance has been avidly anticipated following the Court of Justice for the European Union's ruling in the *Schrems II* case invalidating the EU-U.S. Privacy Shield.

RECENT TROUTMAN PEPPER PRIVACY PUBLICATIONS

- Californians Pass CPRA, Expanding Consumer Protections
- Five Things You Should Know About Tenant Screening
- COVID-19 Headlines FTC's "Green Lights & Red Flags"
- Troutman Pepper Commemorates FCRA 50th Anniversary
- California AG Releases Third Set of Proposed Modifications to CCPA Regulations
- FCC Issues Notice of Proposed Rulemaking on TCPA Exemptions
- FDA Launches Digital Center of Excellence and ONC Updates HIPAA Security Risk Assessment Tool
- Fraud Emerges as Telemedicine Surges: Compliance Guidance for Telemedicine Providers

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber