Articles + Publications | May 2021

More Privacy, Please – May 2021

WRITTEN BY

Mary C. Zinsner | Molly S. DiRago | Ronald I. Raether Jr. | David N. Anthony | Angelo A. Stio III | Ashley L. Taylor, Jr. | Jack Altura | Gerar Mazarakis | Wynter L. Deagle | Charles Glover

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

Federal

- **FTC Publishes AI Best Practices.** Building upon its April 2020 guidance on Using Artificial Intelligence and Algorithms, on April 19, the FTC published new guidance focused on how businesses can promote truth, fairness, and equity in their use of AI. While recognizing the potential benefits of AI, the guidance stresses the need to avoid inadvertently introducing bias or other unfair outcomes. As a basis for its best practices and lessons learned for using AI, the guidance cites a number of other FTC publications and actions, including its report on big data analytics; a hearing on competition and consumer protection issues of algorithms, artificial intelligence, and predictive analytics; the abovementioned 2020 guidance; and various FTC enforcement actions. The FTC's new guidance is available here.

- **DOL Issues New Cybersecurity Guidance for Employers, Plan Administrators, and Workers.** On April 14, the U.S. Department of Labor issued its first-ever guidance on employee retirement plans' cybersecurity duties, providing important standards on how employers and plan administrators should protect data. As the DOL's benefits unit, the Employee Benefits Security Administration provided three-part guidance: one for employers, the second for plan administrators, and the third for workers who participate in the plans. The DOL's continued recognition and incorporation of cybersecurity into government best practices continues to underscore the need for comprehensive cybersecurity protocols for all organizations doing business or handling information electronically.

- **Department of Energy Pulls Grid Supply Ban Amid Cybersecurity Push.** On April 20, as part of a 100-day initiative to bolster security of utility industrial control systems and energy supply chains, the U.S. Department of Energy revoked a December order blocking the "acquisition, importation, transfer or installation" of bulk power system equipment from China and other countries posing a national security risk. While new recommendations and executive actions for energy supply chain security are being developed, the DOE expects that utilities will "continue to act in a way that minimizes the risk of installing electric equipment and programmable components that are subject to foreign adversaries' ownership, control or influence." The 100-day plan is a collaborative effort between the electricity industry, the DOE, and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency to bolster grid security, including identifying and deploying technologies to track and respond to grid threats in real time. The Federal Energy Regulatory Commission expects to serve a role in the initiative. More information can be found here.

- **Bipartisan Bill Aims to Block Data Brokers from Selling to Federal Government.** On April 21, lawmakers proposed bipartisan legislation to prevent the federal government from buying Americans' user data, such as biometrics and location information, from entities obtaining and selling such data without the owner's consent. "The Fourth Amendment Is Not for Sale Act" subjects data brokers to the same disclosure regulations as social media and telecom companies, and it prevents intelligence and law enforcement from acquiring metadata about Americans' international communications to friends and family abroad without FISA oversight. The proposed legislation also removes the attorney general's authority to grant civil immunity for assisting with surveillance not permitted or required by statute or court order. A copy of the bill can be found here.

State

- **North Carolina Proposes New Consumer Privacy Act Bill.** The North Carolina General Assembly introduced the Consumer Privacy Act (CPA) of North Carolina (SB-569) on April 6. The CPA will expand protections to consumers under the North Carolina Identity Theft Protection Act, and it will apply to businesses that control or process the personal data of (1) at least 100,000 consumers on an annual basis or (2) at least 25,000 consumers and derive over 50% of gross revenue from the sale of personal data. Noncompliance with the proposed CPA will expose businesses to risks of large fines up to $5,000 for each violation. The bill's text can be found here.

- **Pennsylvania Proposes New Consumer Data Privacy Act Bill.** On April 7, Pennsylvania legislators introduced the Consumer Data Privacy Act (CDPA) (HB-1126), modeled on the California Consumer Privacy Act. The Pennsylvania bill applies to professional and employment-related information and provides consumers with a private right of action in cases involving nonencrypted and nonredacted personal information resulting from a business's violation of the duty to implement and maintain reasonable security practices and procedures. Consumers can recover statutory damages of no less than $100 and no greater than $750 per incident, as well as injunctive and declaratory relief. Further, the Pennsylvania attorney general can bring civil enforcement actions and seek civil penalties up to $7,500 for each violation. The proposed CDPA text can be found here.

U.S. LITIGATION AND ENFORCEMENT

Standing

- **The Second Circuit Renounces Circuit Split on Standing.** In *McMorris v. Carlos Lopez & Assocs.*,(2d Cir. Apr. 27, 2021), the Second Circuit reconciled rulings from other circuits, formulated its own standing analysis, and concluded the plaintiffs lacked Article III standing. The case involved an inadvertent email by an employee of the defendant, who sent 65 employees a spreadsheet containing sensitive PII (including Social Security numbers and dates of birth) of approximately 130 current and former employees of the company. Three plaintiffs whose information had been disclosed then filed suit with a putative class-action complaint, alleging claims for negligence, negligence *per se*, consumer protection, and other state law claims. The district court concluded the plaintiffs lacked particularized injury, and the Second Circuit affirmed, crafting a three-part test analyzing (1) whether the data has been compromised; (2) whether the data has actually been misused; and (3) the nature of the data at issue and whether it makes it more likely that victims will be subject to future identity theft. Applying these principles, the Second Circuit concluded the plaintiffs failed to show a substantial risk of future identity theft or fraud sufficient to establish Article III standing. A copy of the opinion can be found here.

Arbitration

- **Objectors to Tik Tok Privacy Settlement Push for Arbitration.** On April 2, almost a thousand TikTok users accusing the company of violating the Biometric Information Privacy Act argued that the $92 million settlement would violate the Federal Arbitration Act by blocking their rights to individual arbitration. Should the court grant preliminary approval of the agreement, the plaintiffs asked the court to either explicitly exclude arbitration

claimants or allow them to opt out online or en masse through counsel. The objectors described the current settlement requiring users to opt out individually by physical mail as "burdensome," and it intended "to obstruct and confuse the arbitration claimants into losing their rights without affirmative consent." Attorneys representing the class of plaintiffs who agreed to the settlement in February argued that arbitration claimants lack standing to object because they plan to opt out of the agreement. A copy of the objection to the proposed class action settlement can be found here.

Privacy

- **Spotify Announces It Will Not Use Speech Recognition Patent Due to Privacy Concerns.** Despite being granted a speech-recognition patent earlier this year in January, Spotify recently said that it has no plans to implement it. This comes after digital rights nonprofit Access Now issued a letter, stating that the technology is "dangerous, a violation of privacy and other human rights, and should be abandoned." Access Now shared concerns that the technology could lead to emotion manipulation, gender discrimination, privacy violations, and data security issues. In its response to the letter, Spotify acknowledged that it has "an obligation to innovate responsibly" and wanted to assure the public that any product Spotify develops "will reflect [its] commitment to conducting business in a socially responsible manner."

- **Orange County Transportation Authority Strikes $41M Settlement in Toll Data Privacy Suit.** Drivers who received toll penalties will get their penalties reduced or forgiven as part of the settlement of a lawsuit accusing the agency of illegally sharing PII of motorists and flouting state privacy laws to collect unpaid tolls and fines. The proposed settlement class includes drivers whose PII was provided by OCTA to other agencies, the California Department of Motor Vehicles, car rental companies, and third-party debt collectors. The settlement provides for up to $40 million in penalty forgiveness and $1 million to a cash settlement fund, which will be used to fund cash awards, administration costs, attorney's fees, and a service award to the class representative. The memorandum requesting U.S. District Judge Otis D. Wright II in the U.S. District Court for the Central District of California to grant preliminary approval of the settlement is available here.

Biometrics

- **Plaintiffs in Clearview AI Privacy MDL Seek Preliminary Injunction.** In the Clearview AI MDL privacy litigation, the plaintiffs have moved for a preliminary injunction, alleging violation of the Illinois Biometric Information Privacy Act. The plaintiffs cited a recent patent application and the "backwards" nature of the opt-out process as grounds that the company "can't be trusted," and they argued that the court should enjoin the company from continuing to collect and use biometric data during the pendency of the litigation. This is the second injunction sought against Clearview AI in the litigation pending in the Northern District of Illinois; the company prevailed on the first request by threatening to cut ties with any nonlaw enforcement accounts and implementing a process by which Illinois residents could opt out of its biometric collections.

- **Nursing Staff Agency Settles Biometric Privacy Suit for $5.4M.** Heartland Employment Services LLC, a nursing and rehabilitation care company, agreed to pay $5.4 million to former employees who claimed the company's fingerprint collection violated the Illinois Biometric Information Privacy Act (BIPA). BIPA requires employers to receive workers' informed consent prior to collecting, storing, and using biometric information and mandates a publicly available written description of data retention and destruction practices. In their complaint, originally filed in 2018 in Illinois state court and later removed to federal court, the employees alleged that Heartland collected their fingerprints without first receiving written consent and explicitly disclosing the collection. Under the agreement, Heartland is not required to admit fault or liability.

INTERNATIONAL REGULATION AND ENFORCEMENT

- **European Union Moves to Regulate High Risk AI Use.** On April 21, the European Commission (Commission) published its Proposal for a Regulation on a European Approach for Artificial Intelligence. The Commission

simultaneously proposed a new machinery regulation, designed to ensure the safe integration of AI systems into machinery. Last month the European Union's (EU) executive commission proposed comprehensive regulations aimed in part at curbing abuse of what it considers "high risk" AI systems. As such, the proposal includes rules that restrict the use of AI to pre-screen education, employment, and loan applications that employ subliminal techniques for social manipulation and to exploit children. If approved, these regulations would propel the EU to the forefront of global AI regulation. The proposal also creates a European Artificial Intelligence Board composed of representatives from EU member states and the Commission, which would facilitate a harmonized implementation of the Artificial Intelligence Act, provide advice to the Commission, and share best practices between EU member states. If adopted by the European Parliament and Council, the Artificial Intelligence Act would apply directly across the EU.

CYBERSECURITY TRENDS

- **Almost Half of North America and European Businesses Hit by Cyberattack in 2020.** The Cyber Readiness Report 2021, issued by London-based specialist insurer Hiscox Ltd., found 50% of North American and European companies suffered a cyberattack in 2020 — a 12% rise in attacks from 2019. Although mean cybersecurity defense spending rose $1.8 million over the past two years, Hiscox claims the adoption of cyber insurance is still "patchy." Others question the utility of cyber insurance, saying that paying cyber ransoms only encourages further attacks, and cyber insurance does not substitute robust cyberattack mitigation.

- **Vaccination Passports Debate Continues.** A lack of a federal mandate requiring a single vaccination credential is resulting in a patchwork of state and private-sector practices. Currently, it is unclear how widespread the practice of vaccination verification — such as New York state's application "Excelsior Pass" showing proof of vaccination or a negative COVID-19 result — will be nationally and internationally, and standards will vary. While some companies will require inoculations for staff and customers, most policymaking seeks to ban vaccination requirements. Advocates of vaccination passports argue it is the fastest and safest way to reopen economies, but opponents argue the practice infringes on civil liberties and would delay economic recovery. Moreover, there is no digital standard for inoculation proof, and paper cards are easy to fake. As such, passport advocates seek federal guidelines ensuring health certifications will protect customer privacy and be valid internationally.

TROUTMAN PEPPER TEAM SPOTLIGHT: WYNTER DEAGLE

Wynter Deagle is a trusted advisor in the boardroom and a fierce advocate in the courtroom when businesses face issues found at the intersection of law, technology, and innovation. She is a first-chair trial lawyer who specializes in defending clients from privacy and data security-related consumer class actions and regulatory enforcement matters. Wynter also defends clients in individual and class actions, as well as regulatory enforcement actions asserting deceptive business practices and negligence claims arising out of data security breaches and/or data collection, use, and sharing practices.

Outside of the courtroom, Wynter helps clients navigate the sea of confusing federal, state, and international privacy and data security laws and regulations. Most recently, Wynter has devoted significant time to advising clients on the intricacies of the CCPA and empowering clients to make compliance decisions that balance privacy with business functionality.

A passionate advocate for diversity, equity, and inclusion in the legal and business communities, Wynter holds a Certified Diversity Professional (CDP) designation from the National Diversity Council and regularly provides

advice on the development of DEI plans, inclusive recruiting and talent management strategies, and leadership development programs.

Known for her consummate leadership, Wynter acts as the managing partner of Troutman Pepper's San Diego office, a member of its Diversity Committee, and founded the San Diego office's diverse attorney recruiting program. She also serves as president of the board of directors of Girls, Inc. of San Diego County and as pro bono counsel to SunLaw — an organization dedicated to the promotion and advancement of women in-house attorneys.

In her free time, Wynter is an amateur auto mechanic and restores classic American muscle cars. Her current project car is a 1966 Mustang convertible.

WEBINARS

- **Hot Topics In Privacy Law | Thursday, May 20, 2021 | 8 a.m. ET (5 a.m. PT).** As part of the *New Jersey State Bar Association Annual Meeting*, Troutman Pepper Partner Angelo Stio will serve as a moderator and speaker with fellow panelists the Honorable Ronald Hedges (ret.) and the Honorable Mohammed Sohail (J.S.C.) to discuss Fourth Amendment search and seizure cases involving digital privacy; Fifth Amendment self-incrimination and mandate to turn over passwords; and Article III standing.

- **How 2020 Vision Has Blurred Attorney Client Privilege in Incident Response | Monday, May 17, 2021 | 3:15 p.m. ET (12:15 p.m. PT).** Troutman Pepper Partners Ron Raether and Ashley Taylor will speak on the RSA panel, "How 2020 Vision Has Blurred Attorney Client Privilege in Incident Response," where they will discuss what the law says about attorney-client privilege and what security teams can do from a practical perspective to keep forensic efforts from coming back to haunt them.

RECENT TROUTMAN PEPPER PUBLICATIONS

- Eleventh Circuit Throws Debt Collectors Under the FDCPA Bus for Sharing Account Information with Letter Vendors
- Federal Court Rules Michigan Privacy Law Protects Nonresidents
- Display of Data Symbols Similar to QR Code Visible Through Envelope Window Insufficient to Establish Article III Standing
- Banking Regulatory Agencies Seek Information on Financial Institutions' Use of Artificial Intelligence
- California Supreme Court Confirms Call-Recording Statute Applies to Parties and Nonparties Alike
- Compelling Arbitration: The Eleventh Circuit Court of Appeals Reverses and Remands a District Court Holding Denying Defendant's Motion to Compel Arbitration in an FCRA Case
- Unanimous Court Cuts FTC's Power to Seek Monetary Redress

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management