Articles + Publications | December 2021

More Privacy, Please – December 2021

WRITTEN BY

Molly S. DiRago | Edgar Vargas | Ronald Raether, Jr. | David N. Anthony | Angelo A. Stio, III | Ashley L. Taylor, Jr. | Mary C. Zinsner | Mary Kate Kamka | Lissette Payne | Arien N. Parham | Jack Altura

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

- **Wisconsin Enacts Insurance Data Security Law With Notification Requirements**
  - On November 1, Wisconsin became the latest state to enact a data security law requiring notification in the event of a data security incident. The law requires applicable entities to report insurance-related security incidents within three business days to the state insurance commissioner. The statute is modeled after the Model Insurance Data Security Law and is similar to New York's Cybersecurity Regulation. Click here for a more detailed analysis of the law.

- **CFPB Issues Advisory Opinion on Name-Only Matching Procedures for Entities Involved in Generating Consumer Reports**
  - On November 4, the Consumer Financial Protection Bureau (CFPB) issued an advisory opinion stating that a consumer reporting agency (CRA), which engages in name-only matching violates the Fair Credit Reporting Act's (FCRA) reasonable procedures requirement, 15 U.S.C. § 1681e(b). Although styled as an advisory opinion, the CFPB made clear that the opinion is considered an "interpretive rule" issued under the CFPB's authority to interpret the FCRA. The opinion will be published at 12 C.F.R. Part 1022 and will become effective as of the date of publication. A more detailed analysis of the opinion can be found here.

- **House Representatives Reintroduce Sweeping Online Privacy Act**
  - On November 18, U.S. Reps. Anna G. Eshoo (D-CA) and Zoe Lofgren (D-CA) reintroduced the Online Privacy Act, which would create user data rights, place limitations and obligations on companies that collect and use consumer data, and create a digital privacy agency to enforce privacy laws. Eshoo and Lofgren previously introduced the act on November 5, 2019. Given the rise in digital work and online activities, the bill seeks to "protect individuals, encourage innovation, and restore trust in technology companies." The press

release can be found here.

- **Joint Rule Proposed to Establish Computer-Security Incident Notification Requirements for Bank Service Providers**

  - On November 18, the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (Board), and the Office of the Comptroller of the Currency (OCC), "issued a joint final rule to establish computer-security incident notification requirements for banking organizations and their bank service providers." The letter applies to all FDIC-supervised institutions. Among other provisions, the rule will require: (1) banking organizations to notify the FDIC as soon as possible and no later than 36 hours after determining that a computer-security incident rising to the level of a "notification incident" has occurred; and (2) a bank service provider to notify at least one bank-designated point of contact at each affected customer banking organization as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded covered services for four or more hours. For more information click here.

U.S. LITIGATION AND ENFORCEMENT

- **Apple Files Suit Against NSO Group for Surveilling and Targeting Apple Users**

  - On November 23, Apple filed a federal lawsuit in the Northern District of California against NSO Group and its parent company alleging the company hacked Apple user devices and installed malware and spyware. NSO Group is an Israeli technology firm that designs spyware products for third parties. In the complaint, Apple claims NSO Group developed a spyware known as "Pegasus" to target and attack government officials, journalists, employers, and activists. Pegasus is installed remotely and without consent, and permits surveillance of an owner's activities and communications. Apple claims that "Pegasus can record using a device's microphone and camera, track the phone's location data, as well as collect email, text messages, browsing history, and a host of other information accessible through the device." Apple seeks redress, punitive damages, and a permanent injunction preventing NSO Group from using any of its products on Apple devices.

- **Judge Preliminarily Approves Class Settlement in Dispute Over Fintech Company's Alleged Use of Consumer Data Without Consent**

  - On November 19, a judge in the Northern District of California granted preliminary approval of a class action settlement in a case filed against Plaid Inc. Plaintiffs alleged that Plaid, a fintech company, violated users' privacy rights by improperly accessing and profiting from users' bank credentials and other personal financial information. The $58 million dollar settlement includes injunctive relief provisions that require Plaid to implement business practice changes to remediate the alleged privacy violations and to properly safeguard user's privacy in the future. *See In re Plaid Inc. Privacy Litig.*, No. 20-3056 (N.D. Cal.).

- **CISA Issues Broad Cybersecurity Directive**
    - On November 3, the Cybersecurity and Infrastructure Security Agency (CISA) ordered federal agencies to fix several software and hardware vulnerabilities. Binding Operative Directive 22-01 (the Directive) established a CISA-managed catalog of known exploited vulnerabilities that carry significant risk and establish requirements for agencies to remediate any such vulnerabilities. The Directive requires agencies to review and update internal vulnerability management procedures within 60 days. Recent cyberattacks have prompted CISA to change how it addresses vulnerabilities and to move toward cataloging all known vulnerabilities while requiring federal agencies to quickly provide patching.. The Directive applies only to federal civilian agencies, and excludes the Department of Defense and Intelligence Community.

- **U.S. Lawmakers Ask Facebook to Disclose its Targeted Ads for Teens.**
    - On November 22, U.S. Sen. Ed Markey, (D-Mass.), with Reps. Kathy Castor, (D-Fla.), and Lori Trahan, (D-Mass.) sent a letter to Facebook requesting that it provide its advertising practices targeted toward teens. The letter refers to "new research" suggesting that Facebook targets teens with ads based on their personal information. The letter requests that Facebook "respond to this research, address this apparent inconsistency between the company's promises and its practices, and explain in detail the process by which targeted ads reach teens on its platforms." Among other questions, the lawmakers ask whether Facebook has shared its advertising data with potential advertisers and whether Facebook's advertising system promotes weight-loss and cigarette or alcohol use. Facebook has until December 13, to respond to the letter.

- **FTC Releases Report on Data Privacy Practices of Internet Service Providers**
    - The FTC recently released a report on the data privacy practices of internet service providers (ISPs) from July 2019 to July 2020. The report looks at six ISPs, comprising approximately 98.8% of the mobile internet market, and includes AT&T Mobility LLC, Cellco Partnership dba Verizon Wireless, Charter Communications Operating LLC, Comcast Cable Communications dba Xfinity. and Google Fiber. Noting concerns with the "opacity" of the companies' privacy practices, the report states that "[w]hile several ISPs in our study tell consumers they will not sell their data, they fail to reveal to consumers the myriad of ways that their data can be used, transferred, or monetized outside of selling it, often burying such disclosures in the fine print of their privacy policies." The report also mentions concerns with three additional aspects of the ISP's privacy practices, including illusory choices about the use of personal data, lack of meaningful consumer access to data, and unfettered discretion with data retention and deletion. This report likely highlights the FTC's increased interest in ISP privacy practices going forward.

INTERNATIONAL REGULATION AND ENFORCEMENT

- **UK Supreme Court Finds Data Protection Representative (i.e., Class) Action Cannot Be Pursued Against Google**

- On November 10, the United Kingdom (U.K.) Supreme Court issued a decision in *Lloyd v. Google LLC*, UKSC2019/0213 (Supreme Court of the United Kingdom), a "representative action" on behalf of 4.4 million Google users alleging their internet activity was tracked without their knowledge or consent. The decision held that the loss of control of personal data by consumers alone is insufficient to establish that all claimants had the "same interest." In other words, the Court found that each member of the proposed class would need to prove his/her individual damages, thus precluding the use of a representative action. In this regard, the decision is analogous to many U.S. cases, where courts have rejected as insufficient to satisfy the predominance requirement to certify a class under Fed. R. Civ. P. 23(b)(3). Click here for a more detailed analysis.

- **China's First Full-Scale Data Protection Law Comes into Effect**

  - On November 1, China's Personal Information Protection Law (PIPL) went into effect. Generally, PIPL applies to data processing that occurs (1) to provide products or services to individuals located in China; (2) to monitor/evaluate behavior of individuals located in China; and (3) other circumstances described in laws or administrative regulations. PIPL requires, among other things, a lawful basis for data processing activities and responding to/honoring data subject requests. Notably, PIPL has strict requirements for cross-border transfers, including meeting a "necessity test," giving notice of the transfer, getting consent to the transfer, and meeting one of the following four conditions: (1) obtaining approval from the relevant government authority following a security assessment; (2) obtaining a personal information protection certification from the relevant government authority; (3) executing a contract with the recipient organization containing standard contractual language; or (4) satisfying "other conditions" provided by laws, regulations, or the Cyberspace Administration of China. Fines for violations of the law can include up to $7.7 million, or 5% of a business' revenue from the previous year.

- **European Center for Digital Rights Files EU GDPR Complaint Against Dating App**

  - This month, the advocacy group European Center for Digital Rights (also known as NOYB or None Of Your Business) filed a complaint against the dating app Grindr regarding its user authentication requirements. According to the complaint, the dating app requires users to authenticate their identity by presenting a copy of a government-issued ID or passport, a photograph, and email address, even though the user's account may not contain this information. The complaint alleges that Grindr could simply use the email and password associated with the user's account to authenticate the user's identity, which is far less invasive. NYOB claims that requiring users to provide a photo ID and photograph violates the GDPR's principle of data minimization.

- **Ireland's Data Protection Commission Changes Breach Notification Form**

  - Ireland's Data Protection Commission issued a statement online summarizing recent changes to its breach notification form. Among these changes are: (1) required confirmation regarding whether the breach is likely to result in an increased risk to consumers; (2) new questions concerning whether the breach relates to cross-

border processing; (3) requirements for classification of the controller's industry; (4) new options for specifying the types of data affected by the breach; and (5) requirements to include additional details relating to the technical and organizational security measures at issue in the breach.

TROUTMAN PEPPER TEAM SPOTLIGHT: MARY ZINSNER

Based out of Troutman's Washington, D.C. office, partner Mary Zinsner has over 30 years of experience representing financial institutions in state and federal courts nationwide. Mary has handled every type of litigation impacting financial services and consumers, including claims under the Uniform Commercial Code, Fair Credit Reporting Act, Real Estate Settlement Procedures Act, Truth in Lending Act, Fair Debt Collection Practices Act, Fair Housing Act, Gramm-Leach Bliley Act, Bank Secrecy Act, Racketeer Influenced and Corrupt Organization Act, and state consumer protection statutes. Her experience includes representing banks in class actions, data breach MDLs, and privacy matters.

Banks seek Mary's counseling on matters affecting retail operations and compliance, including issues such as garnishments and pre-litigation disputes. She applies "lessons learned" from litigation to help her clients with all aspects of their daily banking practices. Workable approaches to dispute resolution are considered in every litigation matter.

Committed to cultivating professionalism and education on the rule of law, Mary serves on the Board of Directors of the Virginia Law Foundation. Mary is a former member of the Board of Governors of the Virginia Bar Association, a permanent member of the Judicial Conference of the U.S. Court of Appeals for the Fourth Circuit, and a Master in the Pauline Newman Inn of Court. Mary is proud of her ties to Virginia and is an experienced "Rocket Docket" practitioner, having clerked for the Honorable Claude M. Hilton in the U.S. District Court for the Eastern District of Virginia.

Mary recently joined the American Arbitration Association's Roster of Arbitrators.

On weekends and during her spare time, Mary can be found with her husband at college sporting events. All four of her children played or are currently playing Division I college sports.

WEBINARS

- **Avoiding Ethical Pitfalls with Technology in an Increasingly Remote and Technology-Reliant | Thursday, December 9, 2021 | 2:30 p.m. ET**

Using technology devices and systems in your law practice can be both exciting and daunting. How do you become competent in making those selections and using those technologies? How do you protect client confidentiality and ensure compliance with the Rules of Professional Conduct and privacy laws? Troutman Pepper attorneys Mary Zinsner, Alison Grounds, and Jamie Theriot will use real-life stories to provide tips on how to both prevent potential problems and respond efficiently and ethically when they do occur. For more information, please click here.

- **The Power and Pitfalls of Data: Striking a Balance to Unlock Growth and Future-Proof | Thursday, December 9, 2021 | 4:00 p.m. ET**

  Troutman Pepper Partner Tim Butler will be joined by Christine Boucher of Delta Air Lines and Melati Belot of Y Media Labs for a panel discussion on, "The Power and Pitfalls of Data: Striking a Balance to Unlock Growth and Future-Proof," for a Corporate Counsel Institute CLE.

RECENT TROUTMAN PEPPER PUBLICATIONS

- Think Fast: Banking Regulators Release Final Computer-Security Incident Notification Requirements
- U.K. Supreme Court Finds Data Protection Representative (i.e., Class) Action Cannot Be Pursued Against Google
- Wisconsin Enacts Insurance Data Security Law Requiring Notification of Cybersecurity Incidents to Insurance Commissioner Within Three Business Days

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management