Articles + Publications | September 2021

More Privacy, Please – September 2021

WRITTEN BY

Molly S. DiRago | Ronald Raether, Jr. | Gerar Mazarakis | Ashley L. Taylor, Jr. | David N. Anthony | Angelo A. Stio, III | Graham T. Dean | Jack Altura | Justin Golart | Noah J. DiPasquale

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

- **FCC Takes Further Steps to Root Out Illegal Robocalls.** On August 5, the Federal Communications Commission (FCC) announced further plans to thwart illegal robocalls. The agency is considering rules requiring Voice over Internet Protocol (VoIP) providers to apply for direct access to phone numbers to comply with anti-robocalling obligations, including conditioning a VoIP provider's ability to obtain numbers on commitments that the carrier will not facilitate illegal robocall traffic. New rules also establish an appeal system for voice service providers stripped of their caller ID verification for alleged violations of the FCC's "SHAKEN/STIR" protocols — the FCC's standard for industrywide call authentication. Under the new standard, the digital certificate verifying a call's origin may be revoked if the provider carries robocalls, rendering the calls marked as potential spam. While major U.S. service providers must adopt the SHAKEN/STIR technology by June 30, smaller carriers have an additional two years for implementation. On August 9, a coalition of attorneys general from all 50 states and the District of Columbia asked the FCC to shorten this deadline and require small voice providers to adopt the technology as soon as possible.

- **What to Know About GOP Senators' Latest Data Privacy Push.** Updated versions of the Data Protection Act of 2020 and the SAFE DATA Act have been reintroduced in the U.S. Senate. The first of these reintroductions occurred on June 17 when Senator Kirsten Gillibrand (D-NY) introduced the Data Protection Act of 2021 (S. 2134), which would establish a federal Data Protection Agency (DPA) without creating a comprehensive federal privacy regime. As compared to last session's version, the Data Protection Act of 2021 provides for a stronger DPA and is more prescriptive about the scope of the DPA's authority. The other noteworthy reintroduction occurred on July 28 after Senators Roger Wicker (R-MS) and Marsha Blackburn (R-TN) reintroduced Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act (S. 2499). Unlike the Data Protection Act of 2021, the SAFE DATA Act seeks to establish a comprehensive privacy regime, which would include many of the concepts found in other state and federal privacy bills/laws, such as consent requirements for sensitive data, data subject rights, and privacy policy requirements. The previous version of the SAFE DATA Act merged a discussion draft of the U.S. Consumer Data Protection Act with provisions from the Filter Bubble Transparency (FBT) Act and the Deceptive Experiences to Online Users Reduction (DETOUR) Act. The FBT Act and the DETOUR Act both addressed narrower privacy issues about online consumer manipulation (*e.g.*, via "dark patterns) and had bipartisan support. The latest version of the SAFE DATA Act does not include the provisions from the FBT Act or the DETOUR Act. Finally, it is worth noting that SAFE DATA Act would preempt state laws, while the Data Protection Act of 2021 would not. Thus far, the SAFE DATA Act and the Data Protection Act of 2021 have failed to advance beyond committee assignment. For more information about these Senate bills click here.

- **FTC's Safe Harbor Reduction Fuels Further COPPA Changes.** On August 4, the Federal Trade Commission (FTC) delisted for the first time a safe harbor provider tasked with ensuring companies properly handle children's data under the Children's Online Privacy Protection Act (COPPA). The COPPA safe harbor program allows organizations to develop their own oversight programs that meet or exceed COPPA's protections for children, while deeming companies as certified members compliant with the regulations. The FTC removed Aristotle International, Inc. from the list of self-regulatory organizations after warning earlier this year that Aristotle may not have sufficiently monitored member companies. The FTC considered Aristotle's response to this warning "inadequate," and agency staff planned to recommend revoking its approval of Aristotle's program. On June 1, Aristotle notified the FTC that it was withdrawing from the COPPA safe harbor program. FTC Commissioner Rohit Chopra stated that the FTC could terminate other programs flouting their obligations and enact additional reforms to the safe harbor program, including subjecting safe harbor operators to routine reviews of granting lifetime approval. Aristotle was one of seven self-regulatory organizations the FTC approved over the past two decades.

U.S. LITIGATION AND ENFORCEMENT

- **No Standing in Data Breach Case Involving "Essentially Useless" Stolen Data.** In *Burns v. Mammoth Media, Inc.*, a Central District of California court dismissed a data incident class action for lack of standing because the stolen data was "essentially useless" and not the type that could lead to identity theft and other harms. Mammoth's motion included a declaration from its chief technology officer that the compromised data could not have been used to access social media accounts that were allegedly compromised following the incident. The court accordingly treated Mammoth's motion as a factual challenge to the plaintiff's standing and concluded that the plaintiff did not rebut Mammoth's declaration. The court did not address whether or how *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), affected the plaintiff's allegations of standing based on fear of future harm. The plaintiffs have since amended their complaint, perhaps to address *Ramirez*. For a deeper analysis of *Burns v. Mammoth*, click here.

- **Residents Say Macy's Belongs in Facial-Data Privacy MDL.** On August 6, Illinois residents urged the Northern District of Illinois to reject Macy's Retail Holdings, Inc.'s attempt to evade multidistrict litigation over Clearview AI, Inc.'s facial recognition database. Clearview developed its database by scraping over three billion online photos, including the Illinois residents' photos, and Macy's allegedly accessed Clearview's database over 6,000 times without notice. Residents argued that Macy's actions deprived them of the ability to consent to use of their biometric data and that allowing Macy's to escape the litigation would turn the Illinois Biometric Information Privacy Act (BIPA) into a "toothless tiger." Macy's argued that the residents failed to establish standing to pursue BIPA claims against the department store because it did not upload the residents' photos or cause the residents harm. The spate of lawsuits against Clearview began in early 2020 when an Illinois resident claimed Clearview violated BIPA by failing to obtain informed consent prior to collecting, storing, using, and profiting from the biometric data. The plaintiffs in the Illinois case recently asked the court for an injunction prohibiting Clearview from distributing their personal data, but the court rejected the request on the grounds that the plaintiffs had not demonstrated a likelihood of irreparable harm.

- **Alphabet Board Beats Investors' Child Privacy Suit for Now.** On July 30, the Northern District of California dismissed a 2019 complaint by Alphabet, Inc.'s (which owns YouTube through its subsidiary Google LLC) shareholders, accusing Alphabet's directors of violating COPPA by knowingly collecting children's online data. U.S. District Judge Richard Seeborg stated the shareholders had not met Delaware's corporate law standard that requires showing the directors failed to implement controls or consciously failed to oversee operations. Weeks before the complaint, Alphabet reached a record $170 million settlement with the FTC in light of allegations that YouTube illegally collected children's personal information without parental consent. Judge Seeborg explained that the directors' knowledge of the regulatory investigation did not mean they acted with scienter in allegedly breaching their fiduciary duty. While granting leave to amend, the judge stated it is "far from clear" how the investors might cure the deficiencies in their pleading.

- **Ancestry.com Immune From Privacy Claims for Compiling Database of Yearbook Photos.** The Northern

District of California recently held that Ancestry.com was immune under Section 230 of the Communications Decency Act (CDA), which provides that the provider of an "interactive computer service" cannot be treated as the publisher or speaker of information provided by "another information content provider." The plaintiffs were individuals whose photos, names, and estimated ages were included in Ancestry's Yearbook Database, advertisements, and marketing emails. They argued, in part, that Section 230 immunity did not apply because Ancestry "created content by extracting the yearbook content and using the content in its own webpages and emails," adding information to the content and adding interactive content. Magistrate Judge Beeler rejected this argument, finding that Ancestry did not ***transform*** the content, but "just offered it in a different form," and therefore only acted as a publisher, not a content provider. This case is notable for its broad application of Section 230 protections in the context of an internet platform facing claims based on its compilation and republication of third-party content. The plaintiffs have appealed the case to the U.S. Court of Appeals for the Ninth Circuit. To read more about this decision, click here.

- **Court Rejects Thomson Reuters' Claim of CDA Immunity for CLEAR Product.** On August 16, the Northern District of California denied Thomson Reuters' motion to dismiss claims that its CLEAR product — which compiles dossiers of nonpublic information on individuals aggregated from third-party sources — violated the publicity rights of the plaintiffs by selling their personal information. Thomson Reuters argued, in part, that it was immune from CDA Section 230 claims because it merely compiled information created by other information content providers and therefore could not be treated as the publisher or speaker of such information. Judge Chen held that Section 230 immunity did not apply because Thomson Reuters is "responsible, in whole or in part, for the creation or development of" the dossiers, and thus was the "creator" of the content even though the dossiers consisted only of information from third parties. Judge Chen further reasoned that Section 230's purpose is to immunize the removal of "user-generated content," not the creation of content. "Here, there is no user-generated content — Thomson Reuters generates all the dossiers with the plaintiffs' personal information that is posted on the CLEAR platform." The order notably does not discuss or cite the 2021 *Callahan v. Ancestry.com* case, in which a Northern District of California magistrate judge held that Section 230 immunity did apply to the aggregation and republication of third-party content.

- **Zoom Inks $85M Deal to End Users' 'Zoombombing' Suits.** Zoom recently agreed to an $85 million settlement over a 2020 Northern District of California lawsuit, accusing it of sharing users' personal data to unauthorized third parties, misrepresenting the strength of its encryption protocols, and failing to prevent malicious meeting disruptions. Under the proposed agreement, users with paid subscriptions will be eligible to receive the greater between 15% of their subscription costs during the class period or $25. Zoom also agreed to improve security, privacy disclosures, and consumer data protection through over a dozen major changes to its practices. Such changes include offering specialized training to employees on privacy and data handling, alerting users when hosts or other participants use third-party applications during a meeting, and ensuring its privacy statement discloses users' ability to record or transcribe meetings or share data with third parties.

- **CSX Derails Privacy Claims From Worker Termination Suit.** On August 2, the Southern District of West Virginia dismissed invasion of privacy claims from a wrongful termination suit brought against railroad company CSX Transportation, Inc. by its former employees. U.S. District Court Judge Robert C. Chambers found that the alleged disclosure of data, including unredacted Social Security numbers to chiropractic associations, benefits providers, and the Railroad Retirement Board, was not "sufficiently widespread" — a requirement for bringing an invasion of privacy claim for publicly disclosing private facts in West Virginia. Judge Chambers explained that the plaintiffs had not attempted to quantify the number of people who viewed the data and provided no compelling argument to rebut CSX's claim that the files were only disclosed to those with a legitimate interest in the information.

- **Fifth Circuit Data Hack Ruling May Increase Privacy Litigation.** In late July, the U.S. Court of Appeals for the Fifth Circuit determined that the meaning of the term "publication" in the context of a privacy-related commercial general liability policy includes dissemination of information to a single person. *Landry's, Inc. v. Ins. Co. of the Pa.*, No. 19-20430, 2021 U.S. App. LEXIS 21668 (5th Cir. July 21, 2021). Consequently, the court determined that an insurance carrier had a duty to defend its insured against data breach liability when the policy included coverage for injury arising out of "[o]ral or written publication, in any matter, of material that

violates a person's right of privacy." In this case, the insured's point-of-sale systems were compromised for 18 months without detection, resulting in over $20 million in fines and losses. After the insured was sued for failing to implement and maintain contractual cybersecurity safeguards and the insurer denied coverage, the district court determined that the term "publication" meant dissemination to the public at large instead of a data breach caused by a third party. The Fifth Circuit reversed, ruling that because the liability policy included "oral or written publication, in any manner" in both offenses for privacy and defamation, the term must mean the same and meant dissemination of information to a single person under the defamation tort standard. Moreover, the Fifth Circuit determined that the phrase "in any manner" meant even merely exposing or presenting information to view.

- **Fintech Giant Plaid to Pay $58M to End Privacy Suit.** On August 5, financial services provider Plaid, Inc. agreed to pay a $58 million settlement over a proposed class-action lawsuit, accusing it of unlawfully accessing without consent personal banking information belonging to users of major financial applications like Venmo and Coinbase. Under the deal, Plaid also must make privacy-related changes to its user interface and delete bank transaction data for consumers whose applications did not request the data. If granted, the settlement would resolve claims that Plaid violated users' privacy rights by concealing the way it collects bank login information when consumers sign up to use a payment application partnered with Plaid. Consumers first suing the company in May 2020 accused Plaid of misleading users by creating an interface mimicking the login screens of users' banks.

INTERNATIONAL REGULATION AND ENFORCEMENT

- **DOJ Says SolarWinds Hackers Targeted 27 US Attorneys' Offices.** The U.S. Department of Justice (DOJ) announced that from May to December of 2020, the actors behind the foreign espionage campaign against SolarWinds Corp. compromised the Microsoft email accounts of employees at 27 U.S. attorneys' offices nationally, including the District of Columbia and Eastern and Southern Districts of New York. Though the DOJ did not disclose the breach's impact on pending cases or investigations, or the information accessed, it said that at least 80% of all emails sent, received, and stored by employees at the four New York federal prosecutors' offices were compromised and that other offices across the country "were impacted to a lesser degree." The breach, discovered last December by cybersecurity firm FireEye, also affected government agencies, including the U.S. Department of Homeland Security and an unknown number of private companies. U.S. government officials have attributed the campaign to Russian military intelligence.

- **Irish Data Authority Looks Into FATCA, EU Data Compliance.** On August 6, the Irish data protection authority said it will ensure transfer of financial information to the U.S. complies with European Union data privacy rules. The Data Protection Commission's (DPC) statement resulted from concerns by American citizens living in Europe that agreements permitting the transfer of U.S. citizen information to the U.S. violated the rules. DPC actions include seeking details on any plans to update America's 2012 Foreign Account Tax Compliance Act (FATCA). Americans abroad have been fighting to overturn FATCA, arguing banking rules make it difficult to access basic financial services. FATCA requires foreign financial institutions to disclose information on U.S. citizens' accounts or face a 30% withholding tax on payments from the U.S. The withholding tax has led to claims that foreign banks share customer information with the U.S. government in violation of customers' privacy. Ireland's actions align with the European Data Protection Board's call earlier this year for national data protection authorities to ensure international agreements involving data transfer concluded before May 2016, as well as with the General Data Protection Regulation (GDPR).

- **GOP Wants Former Huawei Unit Put on Trade Restriction List.** On August 6, Republican lawmakers asked the U.S. Department of Commerce to blacklist Honor Device Co. (Honor) — formerly owned by Huawei. In 2019, the U.S. added Chinese tech giant Huawei to an entity list, restricting it from acquiring U.S. software and technology over concerns of Chinese espionage. The lawmakers argued that Huawei divested Honor to evade the export controls and explained that the controls should focus on Chinese "networks and ecosystems" rather than discrete entities. The list is part of intensifying U.S. efforts to block Chinese access to American networks and includes governments, companies, and individuals who have participated in activities

deemed contrary to U.S. foreign policy and national security interests. As part of these efforts, on August 4, the Senate Commerce, Science, and Transportation Committee cleared the Secure Equipment Act of 2021 (Act) to increasingly block Chinese tech giants from U.S. telecom networks. The Act would advance FCC rules developed last year, requiring telecom companies to uninstall and replace hardware from listed companies found to threaten U.S. national security. While current rules apply to equipment purchased with federal funds, the Act directed the FCC to implement new rules categorically blocking firms on a covered equipment or services list from receiving FCC licenses.

- **Lawmakers Want Countries That Support Ransomware Sanctioned.** On August 5, Senators Dianne Feinstein (D-CA) and Marco Rubio (R-FL) introduced the Stop Ransomware Act (Act) that would sanction countries involved in state-sponsored ransomware attacks. The Act would penalize nations harboring or providing support for cybercriminals behind such attacks and require the president to impose sanctions consistent with those levied on state sponsors of terrorism. Critical infrastructure operators, government contractors, and federal agencies also would be required to report ransomware attacks within 24 hours to the Cybersecurity and Infrastructure Security Agency (CISA), which has 180 days to establish the reporting program. The proposed legislation also requires the development of cybersecurity standards for critical infrastructure groups and regulations for cryptocurrency exchanges.

TROUTMAN PEPPER TEAM SPOTLIGHT: RONALD RAETHER

With more than 20 years of experience navigating federal and state privacy laws, Ron Raether leads Troutman Pepper's Cybersecurity, Information Governance, and Privacy team. His involvement in seminal data compliance and data use cases has helped define current standards in several areas of the law. In fact, Ron assisted one of the first companies required to provide notice of a data breach, and he has since successfully defended companies in hundreds of class actions and regulatory investigations. Continuing his involvement in cutting-edge issues, Ron currently leads the defense of several putative class actions, asserting untested and novel claims relying on the California Consumer Privacy Act and other newly enacted laws. He has maintained a Certified Information Privacy Professional (CIPP/US) certification since 2006.

Known as a skilled interpreter between core business issues and information technology, Ron's experiences with data security, data privacy, patent, antitrust, licensing, and contracts, as well as his understanding of technology, has led him to be involved in legal issues that cross normal firm boundaries. Balancing privacy, cybersecurity, and business functionality, his approach to data governance is uniquely designed with clients in mind as he assists them in adapting to the ever-evolving technological and legal landscapes.

Ron represents clients in a broad range of technology and data privacy matters, including data aggregation and analytics, mobile applications, de-identification/anonymization, including correlating data from multiple connected devices, "connected-things (IoT)," electronic crash- and consumer-reporting systems, and payment technologies.

He also advises on pre- and post-incident compliance concerns, ranging from the development of incident response plans and workflows to guiding clients through immediate forensic investigations, coordinating initial crisis management, including navigating clients through the maze of state and federal notification requirements, addressing post-incident aftermath, and responding to regulatory inquiries.

Ron is a PADI certified scuba instructor and teaches students in the waters of his home state California. His instructions to his rescue class students carries over to his teaching of clients on how to prepare for a data incident. Stop, think, and act. Just as you do not want to be 100 feet underwater, have low air, and be without a plan (and muscle memory on how to act), you likewise do not want to figure out how to respond to an incident in the middle of the crisis.

WEBINARS

- **Colorado Privacy Act – What It Means for Businesses | Wednesday, September 8, 2021 | 3 p.m. ET (12 p.m. PT)**
  On June 8, the Colorado legislature passed the Colorado Privacy Act (CPA) to become the third state to enact a comprehensive data privacy law. Join us as we discuss this new law and how it compares to the California Privacy Rights Act and the Virginia Consumer Protection Act. To register, please click here.
- **NetDiligence Cyber Risk Summit | Tuesday, October 5, 2021 | 11:40 a.m. PT | Santa Monica, CA**
  As if a global pandemic and the California wildfires were not enough, 2020 gifted us with case law blurring the lines even further as to when attorney-client privilege applies to incident-response forensics. Join Sadia Mirza as she discusses 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.For additional information or to register, please click here.
- **American Bar Association's Consumer Financial Services Basics Virtual Conference | Thursday, October 21, 2021 | 3:10 p.m. ET**
  Ron Raether will join a panel discussion titled, "Financial Privacy and Data Security," during which the presenters will discuss key restrictions on the use and disclosure of consumer financial information, including the Gramm-Leach-Bliley Act's privacy provisions and the Affiliate Marketing Rule. The panel will also examine federal and state laws, requiring financial institutions to safeguard consumer information and the impact of data security breaches on the financial services industry. For additional information or to register, please click here.

RECENT TROUTMAN PEPPER PUBLICATIONS

- U.S. Senators Reintroduce Privacy Legislation
- No Standing in Data Breach Case Involving "Essentially Useless" Stolen Data
- FFIEC Issues Guidance on Authentication and Access to Financial Institution Services and Systems
- California District Court Holds Section 230 Immunity Bars Claims Against Ancestry.com for Compiling and Republishing Yearbook Photos
- Four Ways Courts Are Approaching High Court's TCPA Ruling
- The Impact of *Schrems II* on EU and U.S. Cloud-Based Services
- Top Takeways From a Year of CCPA Enforcement
- The FBI Warns Lawmakers that Banning Ransom Payments May Backfire

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management