Articles + Publications | November 2021

More Privacy, Please – November 2021

WRITTEN BY

Molly S. DiRago | Mary C. Zinsner | Ronald Raether, Jr. | David N. Anthony | Angelo A. Stio, III | Ashley L. Taylor, Jr. | Mary Kate Kamka | Gerar Mazarakis | Arien N. Parham | Lissette Payne | Kimberly Hughes Gillespie

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

- **Public Tests Begin for Apple's Privacy Report Tool.** According to *TechCrunch*, Apple recently launched the beta version of its "App Privacy Report" feature, enabling iOS users to view how frequently apps request access to sensitive information and where such information is being shared. When enabled by users, the report — located in a device's "Privacy Settings" — creates a list of the applications' activities over the past seven days. Specifically, the report includes details about applications' access to user data, such as contacts, photos, and sensors, including the microphone or location. Mover, a section called "App Network Activity," allows users to view a list of domains with which applications have communicated over the past seven days. Domains include those used by the app to provide functionality in addition to domains from third-party trackers and analytics providers. "Website Network Activity" provides a similar list focused on websites that contacted domains. Apple sees the report as an opportunity to build trust with users by providing transparency.

- **DOJ Announces Cryptocurrency Enforcement Team and Cyber-Fraud Initiative.** On October 6, the U.S. Department of Justice (DOJ) announced two programs, the National Cryptocurrency Enforcement Team (NCET) and the Civil Cyber-Fraud Initiative, to combat illegal cryptocurrency use and cybersecurity-related fraud by government contractors. Specifically, the NCET will handle complex investigations and prosecutions of cryptocurrency misuse, including crimes by exchanges, money laundering, and darknet sales of illegal drugs, weapons, malware, and other hacking tools. The team also will assist in tracing and recovering assets lost to extortion and fraud, including ransomware. Supervised by Assistant Attorney General Kenneth A. Polite Jr., the NCET draws from the Money Laundering and Asset Recovery Section (MLARS) and Computer Crime and Intellectual Property Section (CCIPS) of the DOJ's Criminal Division, as well as from other division sections and experts from U.S. attorneys' offices. The Civil Division's Commercial Litigation Branch, Fraud Section will lead the Civil Cyber-Fraud Initiative, using the False Claims Act to pursue cybersecurity-related fraud by government contractors and grant recipients. The initiative will hold accountable entities or individuals that knowingly provide deficient cybersecurity services or products, misrepresent their cybersecurity protocols or practices, or violate monitoring or incident reporting requirements.

- **Facebook Whistleblower's Congressional Testimony Attracts Attention.** On October 5, former Facebook employee Frances Haugen testified before the Senate Subcommittee on Consumer Projection, Product Safety, and Data Security about Facebook's negative impact on children and adults, calling for congressional action. Haugen told the subcommittee that Facebook is aware that its products "harm children, stoked division, and weakened our democracy," but refuses to make changes that could hurt its profits. She urged Congress to "break out of previous regulatory frames" and pass effective legislation that would address the current internet

climate. The testimony spurred bipartisan unity to regulate Facebook and other social media companies. Subcommittee Chair Senator Richard Blumenthal (D-CT) supported additional federal privacy legislation and amending Section 230, which shields companies from liability. Senator Marsha Blackburn (R-TN), the committee's ranking Republican, accused Facebook of intentionally targeting children under 13 by "evading and working around" the Children's Online Privacy Protection Act. Haugen chose to come forward after working at Facebook for two years as a product manager in Facebook's Civic Integrity Department.

- **FTC Congressional Report Shows Commissioner Split on Privacy and Competition.** In a September 13 report to Congress, the Federal Trade Commission (FTC) announced that it "will spend more time on the overlap between data privacy and competition," recognizing that many of the largest digital market players acquired their power by their access to and control over user data. "Companies should not only have to stop their illegal conduct, they should not be allowed to gain a competitive advantage by benefiting from data they collected unlawfully," the report stated. Suggesting the commission has a "structural advantage" over its counterparts in other jurisdictions that exclusively focus on data protection or antitrust, the FTC said that its "dual missions can and should be complimentary," making sure it looks at issues arising in digital markets "with both privacy and competition lenses." The report follows aggressive efforts by new FTC Chair Lina Khan to thwart possible anticompetitive conduct and violations of consumer protection law. Commissioner Noah Joshua Phillips dissented, explaining that the report "overstates the synchrony between competition and privacy" and "suggests misplaced priorities, a disregard for statutory boundaries, and the replacement of market preferences with regulatory fiat." Similarly, Commissioner Christine S. Wilson dissented in part, stating that "the FTC must respect both the mandates that Congress bestowed on the agency and the statutory divide between its competition and consumer protection authorities." Countering these views, Commissioner Rebecca Kelly Slaughter said that the FTC has the necessary rulemaking authority, but it has failed to use it. Moreover, Chair Kahn said that understanding "the overlap between data privacy and competition," as stated in the report, "reflects the growing recognition that persistent commercial data collection implicates competition as well as privacy." "In particular," she explained, "concentrated control over data has enabled dominant firms to identify and thwart emerging competitive threats. Monopoly power, in turn, can enable firms to degrade privacy without ramifications." Asserting enforcers across the board have underappreciated the competitive significance of data, "breaking down siloes to better grasp these interconnections is key to ensuring rigorous analysis and effective enforcement," said Kahn.

- **FTC Strengthens Security for Consumer Financial Information and Enforcement Against Dark Patterns.** On October 27, the FTC announced an updated rule, strengthening the data security safeguards financial institutions must institute to protect consumers' financial information. Under the updated Safeguards Rule, nonbanking financial institutions — including mortgage brokers, payday lenders, and motor vehicle dealers — must develop, implement, and maintain a comprehensive security system. Institutions also must explain their information sharing practices, such as the administrative, technical, and physical safeguards used to "access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customers' secure information." Institutions also must designate a single qualified individual to oversee information security programs and periodically report to the board of directors or senior officer in charge of information security. The day after announcing its Safeguards Rule update, the FTC issued a new enforcement policy statement, warning companies against deploying illegal dark patterns that trick or trap consumers into subscription services. The agency acknowledged that it increased its efforts in response to a rising number of complaints about the financial harms caused by deceptive sign-up tactics. According to the agency, its policy statement "puts companies on notice that they will face legal action if their sign-up process fails to provide clear, up-front information, obtain consumers' informed consent, and make cancellation easy."

- **"Higher-Risk" Railway Transit Systems Face New Cybersecurity Requirements.** On October 6, during a keynote address given at the *12th Annual Billington Cybersecurity Summit*, Department of Homeland Security (DHS) Secretary Alejandro Mayorkas announced that the Transportation Security Administration (TSA) will issue new cybersecurity directives for major railroad and rail transit systems, effective later this year. The regulations will require "higher-risk" rail and subway systems, such as Amtrak and those found in large metro areas, to name a cybersecurity official, inform the government of cyberattacks, and implement recovery plans for future attacks. "Taken together, these elements — a dedicated point of contact, cyber incident reporting, and

contingency planning — represent the bare minimum of today's cybersecurity best practices," Mayorkas said. The requirements come after the Colonial Pipeline attack and the computer breach at New York's Metropolitan Transportation Authority that occurred earlier this year. TSA will issue different guidelines to "lower-risk" companies but will only suggest, and not require, compliance. The rail industry is not the only business receiving new instructions; TSA is also improving the cybersecurity for airports and airlines. Mayorkas stated that "there is no better example of how the cybersecurity threat can impact our lives than in the transportation sector and how people commute, see one another, engage with one another."

U.S. LITIGATION AND ENFORCEMENT

- **North Dakota Hires Chief Data Officer.** On November 1, Ravi Krishnan became North Dakota's second-ever chief data officer. According to a press release, Krishnan will be in charge of data science, data management, and developing an applications suite for state agencies; brings two decades of private sector experience; and plans to spread awareness of strong data governance practices among the agencies. Krishnan told *Government Technology* that his efforts will involve a broader look at what counts as data management, addressing the applications drawing on the data, and how these apps are developed and deployed. He wants all agencies to have a comprehensive understanding of their data and its management, including knowledge of what they collect, how sensitive is the collected data, and who is responsible for maintaining and protecting the data. Moreover, Krishnan wants to ensure that agencies have access to necessary data, and his first 100 days will involve studying the department's existing data governance and management plans. Krishnan's previous roles include serving as head of analytics and decision transformation at TransUnion, head of enterprise data architecture and strategy at Discover Financial Services, and consultant to entities in the U.S. and Canada.

- **Automotive Data Company Denied Injunction Against Consumer Privacy Statute.** On October 25, the Ninth Circuit Court of Appeals affirmed the U.S. District Court for the District of Arizona's decision to deny automotive data and software company CDK Global LLC's (CDK) request for injunctive relief against Arizona's new consumer privacy statute. The statute seeks to strengthen privacy protections for consumers whose data is collected by car dealers, and it restricts anticompetitive business practices by technology companies providing database services for dealers. Specifically, the law prevents companies like CDK from limiting access to dealer data by dealer-authorized third parties and requires providers to create a standardized framework to facilitate such access. While CDK argued that the Copyright Act preempted the law because the new law would permit dealers to access CDK's systems and create unlicensed copies, the Ninth Circuit said CDK can comply with the law without having to create a new copy of its software for third-party requests. The Ninth Circuit also said that CDK failed to establish that copies would infringe its reproduction rights. Moreover, the Ninth Circuit disagreed with CDK's argument that the law violates the U.S. Constitution's contracts clause because CDK did not show that the statute impairs its ability to perform its contracts. Lastly, the Ninth Circuit agreed with the District Court's finding that CDK could both comply with the statute's mandate and fulfill its data security obligations. There is "no basis to question the judgment of the Arizona Legislature that the statute promotes the common good through the advancement of consumer privacy and competition," the court said.

- **Preliminary Approval for $92 Million TikTok Settlement.** On September 30, U.S. District Judge John Lee of the Northern District of Illinois granted preliminary approval of a $92 million settlement, resolving the multidistrict litigation *In re: TikTok, Inc., Consumer Privacy Litigation*, which alleged that TikTok violated U.S. privacy law by secretly harvesting and profiting from biometric data, geolocation information, PII, and unpublished digital recordings. Overruling objections, including that minors under 13 should receive unique relief and that the settlement amount failed to reflect the strength of the case, Judge Lee found that the deal between TikTok and approximately 89 million of its users was fair, particularly given risks involved with litigating the claims. For example, among TikTok's "many colorable defenses" was that class members are subject to the class-action waiver and arbitration agreements incorporated in the app's terms of service. The judge explained that if the defendants succeeded on this front, the plaintiffs "would likely receive nothing" given the prohibitive time and expense of undertaking millions of individual arbitrations. Moreover, the defendants confirmed through discovery that the app was not used to collect biometric information.

- **Marriott Kicks Data Breach Stockholder Suit on Statute of Limitations Grounds.** On October 5, Vice Chancellor Lori W. Will of Delaware's Chancery Court found that a 2019 derivative stockholder action, accusing Marriott Corp. directors of failing to protect the company from a large data breach, was barred by a three-year statute of limitations. Marriot stockholder Firemen's Retirement System of St. Louis sued the board, following Marriott's $13 billion acquisition of Starwood Hotels and Resorts Worldwide, Inc. in 2016. The breach, uncovered after the acquisition, exposed personal information of 500 million guests and allegedly led to billions of dollars in damages to Marriott's reputation, business standing, and goodwill. After analyzing each issue, Vice Chancellor Will explained that while "none of the post-acquisition board members face a substantial likelihood of liability for a non-exculpated claim, … [a]ny claim based on pre-acquisition diligence is time-barred." In her ruling, the vice chancellor also added that the suit failed to illustrate the sort of willful failures to act or disclose that would justify stockholder takeover of derivative claims without first putting them to the company board or show that a majority of board members faced too great a liability risk to fairly consider the demand.

- **Southwest Airlines Wins Preliminary Injunction to Stop Kiwi.com From Scraping Flight Data and Selling Tickets.** On September 30, U.S. District Judge Ada Brown of the Northern District of Texas granted an injunction and ordered Kiwi.com to temporarily cease scraping and publishing flight data from Southwest Airlines and selling Southwest flights. Judge Brown found that Kiwi entered a valid contract when purchasing flights on Southwest's website and breached the terms by scraping and presenting Southwest flight data, as well as selling Southwest flights without authorization. Southwest sued Kiwi in January 2021 for breach of contract, violation of the Computer Fraud and Abuse Act (CFAA) by "bypassing Southwest's security systems intended to block automated traffic, or 'bots,' from using its website," and violations of the Lanham Act and Texas statutory laws through use of automated bots for largescale information extraction from Southwest's site, ticket purchases, and ticket resale to over 170,000 customers. At the preliminary injunction stage, Judge Brown found that Southwest proved that Kiwi's sales posed a significant disruption to its customer operations, and Kiwi did not prove that the injunction would significantly threaten its business. While the Texas court's decision illustrates that website owners are successfully bringing non-CFAA claims — most notably breach of contract claims, as means of preventing web scraping — ambiguity remains as to whether the "gates up-or-down" approach to determining CFAA liability depends on contractual limitations in addition to technological barriers. The Supreme Court declined to directly address this issue in its recent *hiQ v. LinkedIn* case, in which it vacated and remanded the Ninth Circuit's decision to enjoin LinkedIn from preventing hiQ from scraping LinkedIn members' public profile data under the CFAA. On remand, a Ninth Circuit panel signaled that it would reaffirm its prior position.

- **Google Settles 11-Year-Old Privacy Class Action.** On October 6, Google informed the Northern District of California that the parties reached a settlement in a class action, where the tech giant is accused of divulging users' search terms. The joint filing did not reveal the terms of the settlement, and the agreement comes after previously reached settlements in 2013 and 2015. The procedural history for the case is circuitous as it was filed in 2010, appealed to the Ninth Circuit twice, and granted certiorari once. The case arises from allegations that Google violated its users' privacy rights by disclosing personal data to other third-party websites. In 2015, the case settled for $8.5 million, however, class members argued over the allocated funds of the cy pres recipients. Then in March 2019, the Supreme Court vacated the settlement and remanded the case to the trial court to evaluate the plaintiffs' Article III standing, considering its decision in *Spokeo, Inc. v. Robins*. Once remanded, Google filed a motion to dismiss, challenging the plaintiffs' standing, but the District Court denied the motion, finding the users had a "substantive right" to privacy.

- **Identical BIPA Complaints Filed Against Walmart and NextGen Hotels.** On October 21, almost identical class-action lawsuits were filed against (1) Walmart, Inc. and (2) NexGen Hotels Management, Inc. and Genuine Hospitality LLC d/b/a TownePlace Suites, alleging breaches of Illinois' Biometric Privacy Act (BIPA) for unlawfully collecting and disclosing employee fingerprints used for timekeeping purposes. Specifically, the plaintiffs' claims included a failure to disclose the purposes for collection and use of the biometric data, failure to inform employees of the disclosure of their fingerprints to third parties, and failure to develop or adhere to a written retention schedule and guidelines. Notably, both complaints reference Illinois precedent established by *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, which held that actual damages are not necessary to bring a valid BIPA claim.

INTERNATIONAL REGULATION AND ENFORCEMENT

- **Global Forum of Bankers Calls for Standardized Cyber Incident Reporting.** On October 19, the Financial Stability Board (FSB), a global forum of central bankers, published a report, finding that jurisdictional differences in cyber incident reporting could damage the financial industry's stability and urging the sector to develop a standardized reporting method. Specifically, the FSB found that jurisdictions are fragmented in terms of what should be reported, methodologies to measure incident severity, reporting timeframes, and use of incident information. The report explained that harmonizing incident reporting would promote financial stability by enabling a common method for monitoring cyberattacks targeting finance, support effective cyber risk supervision among financial institutions, and promote information sharing across jurisdictions.

- **Data Protection Commissioner OKs Processing Data Without Consent.** On October 6, in a preliminary decision shared with data protection authorities across the European Union (EU), Ireland's Data Protection Commissioner (DPC) Helen Dixon said that Facebook does not need consent to process data of European users if the users agree to terms of service. Dixon found that Facebook's terms of service do not illegally force users to consent to data processing as a condition of using the platform. Rather, the General Data Protection Regulation (GDPR) permits companies to legally process such data without seeking user consent by having users agree to a contract, the DPC's office wrote. Explaining that Facebook did not seek to rely on consent to justify its data collection, Dixon said that "[t]he GDPR does not set out any form of hierarchy of lawful bases that can be used for processing personal data." Dixon proposed that Facebook pay a fine between $32 million and $42 million for not clearly communicating to users that it was not asking for their consent as a legal basis for collecting their personal data. Members of the European Data Protection Board will have an opportunity to comment on the Irish DPC's decision before it is finalized. Privacy advocates criticized the decision as allowing companies to bypass EU privacy laws by relabeling data use agreements as contracts.

- **"Moment of Convergence" for US and EU Antitrust Policy.** At an October 1 *Fordham International Antitrust Law and Policy Conference* in New York, European Commission Executive Vice President Margrethe Vestager, Europe's top antitrust official, said in a speech that the past few years have witnessed a "growing convergence between" U.S. and EU "policies and rules" related to market competition. Stating that "Europe and America have a huge amount in common," including shared values and similar challenges of securing supply chains, finding a human-centered approach to new technologies, and maintaining a fair and open world economy, Vestager said that Europe sees many familiarities in current congressional legislation attempting to overhaul U.S. enforcement and the priorities of President Biden and new FTC Chair Lina Khan. Vestager continued by saying that as both the U.S. and EU consider new rules to curb major tech platforms and to address the digital economy and environmental policy, and given the increasing convergence between rules and policies, "now is the time to cooperate even more closely than we've done before." "This moment of convergence is a moment of opportunity," she said, requiring increased cooperation not just in discussing cases, but in regular policy meetings between heads of authorities. Vestager delivered her remarks two days after U.S. and EU officials signaled a potential synchronization of data governance policies on competition, privacy, and telecommunications, among others.

- **Advisory Issued on BlackMatter Ransomware Attack.** On October 18, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA) (collectively, "Agencies) shared an advisory, asking organizations to assist them in reducing their risk of a BlackMatter ransomware attack. BlackMatter is a "ransomware-as-a-service tool that allows the ransomware's developers to profit from cybercriminal affiliates who deploy it against victims." The Agencies' advisory offers technical details, detection signatures, and cyber risk mitigation techniques. With the evolving nature of criminal actors in 2021, the Agencies advise organizations that they should:
    - Implement and enforce backup and restoration policies and procedures;
    - Use strong, unique passwords;
    - Use multifactor authentication; and
    - Implement network segmentation and traversal monitoring.

For additional technical details about BlackMatter, click here.

- **White House Issues Joint Statement on Summit Addressing Ransomware.** On October 14, the White House announced that representatives of 32 governmental entities virtually met to "discuss the escalating global security threat from ransomware[.]" The meeting focused on employing "immediate action" to address the abuse of financial mechanisms to launder ransom payments internationally. The meeting also addressed possible policy frameworks that could "dramatically reduce the likelihood of a ransomware incident," such as by maintaining backups, ensuring software patches are up to date, and educating individuals on mitigating cyber risks. To read the complete statement, click here.

- **EU Justice Commissioner Sees "Good Evolution" on Data Discussions with US.** According to *The Washington Post*, EU Justice Commissioner Didier Reynders met with U.S. regulators in Washington in mid-October, and said the two sides are making "real improvement" on issues, including striking a new deal on transnational data flows to replace the EU-U.S. Privacy Shield. According to Reynders, "[w]e will try to see if it's possible to have a political, clear vision before the end of the year." Efforts include defining the necessity and proportionality of data access, safeguarding the data, and enforcing individual rights. To read Commissioner Reynders's full remarks, click here.

TROUTMAN PEPPER TEAM SPOTLIGHT: KIM GILLESPIE

Health Sciences Transactional Counsel Kimberly (Kim) Gillespie resides in the firm's Richmond office, where she handles a wide variety of health care regulatory work, including privacy and security matters involving the Health

Insurance Portability and Accountability Act (HIPAA), the California Confidentiality of Medical Information Act (CMIA), and the California Consumer Privacy Act (CCPA).

Before joining the firm in January 2020, Kim worked as chief counsel for the University of California San Diego Health (UCSD Health) and also served as UCSD Health's compliance and privacy officer. These roles gave Kim a unique understanding of her client's business operations and the challenges they face on a day-to-day basis — an insight that drives her distinct client approach today.

In her free time, Kim enjoys spending time with her family and trying to keep up with her two-year-old grandson, who is always up for an adventure!

WEBINARS

- **A Day in the Life of a Mock BEC Scam: Learning How to Prevent, Respond, and Recover from Wire Fraud | Tuesday, November 16, 2021 | 3 – 4 p.m. ET**

  Although ransomware continues to make headlines in 2021, business email compromise (BEC) scams remain as one of the top five causes of loss at small and medium-sized enterprises. Join us as we walk through a mock BEC scam in the context of wire fraud, while answering your top questions on to how to prevent, respond, and recover from BEC scams. To register, please click here.

RECENT TROUTMAN PEPPER PUBLICATIONS

- Oregon Attorney General Reports Rise in Data Breaches
- California Privacy Protection Agency Begins to Take Shape
- JPML Articulates Limitations for Consolidation in Geico Data Breach Litigation
- Illinois, We Have a Problem: Judge Refuses to Dismiss IRPA Privacy Claim Against RocketReach
- App Store 'Nutrition Labels' Raise New Privacy Risks for Cos.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management