Articles + Publications | August 2021

More Privacy, Please – August 2021

WRITTEN BY

David N. Anthony | Molly S. DiRago | Ronald I. Raether Jr. | Ashley L. Taylor, Jr. | Daniel Waltz | Angelo A. Stio III | Jason J. Moreira

Authors:
Molly S. DiRago
Jason J. Moreira
Daniel Waltz
Ronald I. Raether Jr.
David N. Anthony
Angelo A. Stio III
Ashley L. Taylor, Jr.
Jessica Ring*
Audra Goldstein*

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

- **Connecticut Passes Stronger Data Breach Notification and Cybersecurity.** The Connecticut legislature recently enacted a pair of new data breach and cybersecurity statutes that will expand notice obligations for businesses subject to data security incidents and incentivize the adoption of industry-recognized cybersecurity standards to protect personal information. Effective October 1, the two statutes will collectively (1) expand the definition of "personal information," (2) shorten the notice deadline from 90 to 60 days after discovering the breach; (3) exempt HIPAA/HITECH compliance companies from the new notice requirements under certain circumstances; and (4) insulate businesses from liability for punitive damages for certain tort claims, provided they can demonstrate compliance with one or more industry-recognized cybersecurity frameworks. Connecticut's passage of the two statutes is consistent with a growing trend of states seeking to tighten their data breach and cybersecurity laws, while simultaneously encouraging and rewarding the adoption of standardized compliance protocols. To read more about these statutes, click here.

- **FBI Recommends No Ban on Ransomware Payments.** FBI Cyber Division Assistant Director Bryan Vorndran advised U.S. legislators not to prohibit ransomware payments. While the FBI discourages victims from paying ransomware demands, Vorndran says banning ransom payments could backfire. If paying ransom were illegal, companies that felt they had no choice but to pay could end up being targeted for a second extortion — for

illegally paying and not reporting the ransom demands. Above all, the FBI highly encourages victims of ransomware attacks to report such incidents to allow the FBI to "identify, pursue, and impose consequences" on the criminal actors. Banning ransom demand payments could undermine these efforts.

- **Strict Facial Recognition Ban in Baltimore.** Recently, Baltimore passed Council Bill 21-0001, prohibiting any person, private entity, or government entity within the city from utilizing facial biometrics. Although other states and cities have enacted laws that directly target facial recognition technology, Baltimore's ordinance takes a stricter stance, imposing criminal penalties of up to $1,000 and potential jail time for violating the ban. The ordinance is currently awaiting Baltimore Mayer Brandon Scott's signature. Once signed, the ordinance will go into effect 30 days after its passage.

- **Executive Order Signals Significant Changes for Technology Manufacturers: FTC's 'Nixing the Fix' Offers Insight into Ramifications of Presidential Directive.** The FTC recently provided a report to Congress, titled *Nixing the Fix*, which offers a roadmap of specific actions the FTC will likely take in response to President Biden's directive. In *Nixing the Fix*, the FTC emphasized that it will enforce existing laws (including the Magnuson Moss Warranty Act, Sherman Act, and FTC Act), engage in targeted rulemaking to clarify prohibitive conduct for manufactures under existing law, and prepare rules to promote consumer education on the repairability of products purchased (similar to the universal calorie labeling for manufactured food products). To read about these issues more in depth, click here.

- **House Passes Bills to Combat Energy Cybersecurity Attacks.** On July 19, the U.S. House of Representatives passed two bills — H.R. 3119, the Energy Emergency Leadership Act, and H.R. 2931, the Enhancing Grid Security through Public-Private Partnerships Act — both aimed to protect critical energy infrastructure. The House introduced H.R. 3119 in the wake of recent, devastating ransomware attacks, like that on Colonial Pipeline, to better address ongoing threats on energy systems. H.R. 2931 requires the Department of Energy to collaborate with a "diverse array of stakeholders" and create a plan to better address the "physical" and "cyber" security needs of utility producers.

U.S. LITIGATION AND ENFORCEMENT

- **American Airlines BIPA Suit May Be Remanded to State Court.** Customers allege that American Airlines violated Section 15(a) of the Illinois Biometric Information Privacy Act (BIPA) by failing to create publicly available biometric retention and destruction schedules. The suit was originally brought by an employee alleging that the airline's fingerprint scanning violated BIPA. The third amended complaint, however, substituted a new class representative and now focuses on the airline's customer service hotline, alleging that it unlawfully analyzes and stores customer voiceprints. The plaintiffs have filed a motion to sever and remand the amended claim to state court. Because the legal landscape on federal standing for BIPA Section 15(a) claims is murky, we will continue to watch this case closely.

- **Cyberattack on Kaseya May Lead to Class Action Lawsuits.** Kaseya, a Miami-based software vendor, was recently attacked by cybercriminals, who targeted Kaseya's virtual systems/server administrator with ransomware. Up to 1,500 organizations are believed to have been impacted by the cybersecurity incident. As of

July 26, Kaseya has confirmed, “in no uncertain terms,” that it did not pay the ransom to the cyberattacker. We expect to see numerous class action lawsuits filed in the near future against Kaseya and the many companies impacted by the incident. To read more about this and the recent legislative response to ransomware attacks, click here.

INTERNATIONAL REGULATION AND ENFORCEMENT

- **Facebook’s Use of WhatsApp Data Is Under Irish Investigation.** On July 15, the European Union’s (EU) data protection authorities directed authorities in Ireland to investigate how Facebook uses personal information from its WhatsApp subsidiary. The investigation spurs from warnings from the Hamburg commissioner for data protection and freedom of information, who back in May announced a three-month ban to prohibit Facebook from processing personal data from WhatsApp. The German commissioner brought the case to the EU data protection authorities to make the ban binding at the EU level. However, EU authorities declined to impose an EU-wide ban. But, given the EU’s position that a “high likelihood of infringements” by Facebook with WhatsApp data occurred, EU authorities are further investigating the matter through the Irish Data Protection commissioner. The announcement by the European Data Protection Board can be read here.

- **US Doubles Sanctions on Russian Cybersecurity Organizations.** On July 16, the U.S. Department of Commerce blocked shipments of advanced technology to several Russian organizations, redoubling the sanctions on the entities already blacklisted by the U.S. Treasury Department earlier in the year. The sanctions stem from President Biden’s executive order, Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation, issued in response to Russian election interference, the high-profile SolarWinds cyberattack, and human rights abuses. The Russian organizations banned by both the U.S. Department of Commerce and the Treasury Department include three joint-stock companies, two intelligence-linked organizations, and at least one Black Sea military installation.

- **Apple Wins Privacy Battle in China Against Third-Party Tracking Systems.** On July 4, *Financial Times* announced Apple’s significant victory against Chinese tech companies attempting to circumvent Apple’s global privacy policies. Last year, Chinese tech groups (led by Baidu, Byte-dance, and two government-affiliated organizations) developed a tracking system, CAID, that would allow them to identify users for targeted advertising even if those users refused to let apps use Apple’s official identification program, IDFA. Beginning in March 2021, Apple responded by blocking updates to apps caught implementing CAID in the App Store. As a result of Apple’s approach, the CAID project failed to gain traction and fizzled out. Spokespersons for some companies involved in developing CAID claim they believed they had Apple’s approval for the project, while quoted privacy consultants believed that the groups simply believed that Apple would not or could not block all offending CAID apps once the technology was disseminated.

- **US State Department Offers $10 Million Bounty to Catch Hackers.** On July 15, the State Department announced its Rewards for Justice (RFJ) Program, which offers rewards of up to $10 million for information to help identify or locate hackers targeting the U.S., while acting at the direction or control of foreign governments

in violation of the Computer Fraud and Abuse Act (CFAA). The agency specifically seeks to target malicious actors for ransomware attacks, extortions, and unauthorized transmission of data from protected computers, including U.S. government and financial institution computer systems. The Rewards for Justice Program has paid out over $200 million in awards since its establishment in the 1984 Act to Combat International Terrorism.

TROUTMAN PEPPER TEAM SPOTLIGHT: PETER WAKIYAMA

Philadelphia Partner Peter Wakiyama serves as a trusted legal advisor to clients in multiple industries with a diverse range of intellectual property, technology, and data privacy and security-related needs. He brings nearly three decades of experience in emerging technologies and has substantial experience handling a wide range of data transactions, such as licensing, strategic alliances, development, and data security and governance. He also provides specialist support for M&A intellectual property and data privacy and security needs. In addition to his legal service offerings, Peter offers a wide range of legal training for clients on a variety of topics, such as data law, SaaS transactions, and open-source software.

A substantial and growing portion of Peter's practice surrounds the intersection of intellectual property, technology, and data, which all require integrated legal consideration. When counseling clients and handling technology transactions, Peter carefully assesses the nature of the data and treats it as a strategic intangible asset where appropriate. His assessment of legal and regulatory compliance requirements, along with a proper intellectual property assessment of the data, routinely results in enhanced value for the client and additional business opportunities.

Peter's reputation in multi-industry emerging technologies and his prior work within the technology industry on early internet technologies have branded him as a go-to resource for clients. We encourage you to reach out and connect with Peter!

WEBINARS

- **COPPA's Next Act: Everyone Is Eager to Protect Children's Privacy | Wednesday, July 28, 2021**

  In this webinar, Troutman Pepper Partner Tim Butler and Associates Chelsea Lamb, Carlin McCrory, and Matthew White provided real-world guidance on the Children's Online Privacy Protection Act (COPPA or Act), including pro-tips for complying with the Act, trends emerging from government enforcement actions and private litigation matters, and recent legislative and regulatory efforts to strengthen privacy protections for children. To watch the recording, click here.

Please also watch out for our invitation to our upcoming Colorado Privacy Act (CPA) webinar on August 31.

RECENT TROUTMAN PEPPER PUBLICATIONS

- 5 Questions on Standing in the Wake of TransUnion
- New Standard Contractual Clauses Supply Opportunities and Obligations for Organizations Transferring Personal Data Out of the EU
- Connecticut Passes Stronger Data Breach Notification and Cybersecurity Liability Statutes
- Colorado Governor Signs Comprehensive Data Privacy Bill — How Does It Compare to California and Virginia?
- Florida's New TCPA Law Effective July 1
- CFPB Issues Bulletin on Rental Screening and Issues of Concern
- Lawmakers Aim to Limit Ransomware Response Options

**Jessica Ring and Audra Goldstein are 2021 summer associates with Troutman Pepper and not licensed to practice law in any jurisdiction.*

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management