Articles + Publications | June 2021

More Privacy, Please – June 2021

WRITTEN BY

Molly S. DiRago | Ronald Raether, Jr. | David N. Anthony | Angelo A. Stio, III | Ashley L. Taylor, Jr. | 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

- **U.S. Treasury Proposes Cryptocurrency Reporting Requirements.** On May 20, the U.S. Department of the Treasury released a new report titled The American Families Plan Tax Compliance Agenda (the "Report) as a supplement to President Biden's American Families Plan. In addition to other tax compliance initiatives, the Report proposes requiring that any cryptocurrency transaction of $10,000 or more be reported to the Internal Review Service (IRS). The Report does not fully detail the cryptocurrency reporting requirements. It does, however, indicate that cryptocurrencies, cryptoasset exchange accounts, and payment service accounts that accept cryptocurrencies would be covered and that businesses receiving cryptoassets with a fair market value of more than $10,000 would be required to report these transactions to the IRS (similar to cash transactions of the same amount). Many of the proposals advanced in the Report will require Congressional approval. To read the Report, click here.

- **New York City Enacts Biometrics Law for Food and Drink Establishments, Entertainment Venues, and Retail Stores.** Effective July 9, food and drink establishments, places of entertainment, and retail stores in New York City that collect, retain, convert, store, or share "biometric identifier information" (*e.g.*, retina or iris scans, fingerprints, voiceprints, and hand scans) from customers must post clear, conspicuous notices near all customer entrances to their facilities. These businesses will also be barred from selling, leasing, trading, sharing, or otherwise profiting from such biometric identifier information. The law gives aggrieved customers a private right of action, subject to a 30-day notice and cure period, with damages ranging from $500 to $5,000 per violation, along with attorneys' fees.

- **Senators Reintroduce Bipartisan Social Media Privacy Protection and Consumer Rights Act.** On May 20, a bipartisan group of senators reintroduced the Social Media Privacy Protection and Consumer Rights Act that would require big tech companies to afford consumers greater control over their data. The act applies to "online platforms," which includes all web applications, public-facing websites, and social and ad networks. While the act would not create a private right of action or preempt state privacy laws governing online platforms, it would be enforced by both the Federal Trade Commission (FTC) and state attorneys general. The act's requirements for online platforms include notifying consumers of any privacy violation or security breach within 72 hours; providing consumers with the right to access their personal data, the right to opt out of the collection and use of their data, and easily accessible privacy disclosures; and establishing and maintaining a privacy program audited at least once every two years.

- **Biden's Executive Order Aims at Improving Cybersecurity.** On May 12, President Biden issued an Executive Order on Improving the Nation's Cybersecurity to boost government action and partnership with

the private sector. Requirements include improving information sharing, infrastructure, detection, investigative and remediation capabilities, and supply chain security, in addition to standardizing federal responses to cybersecurity vulnerabilities and incidents. Moreover, the order requires establishing a Cyber Safety Review Board to review and assess threat activity, vulnerabilities, mitigation activities, and agency responses. Agencies have from 45 to 120 days to begin implementing many of the order's requirements.

- **Senators Introduce Children and Teens' Online Privacy Protection Act.** On May 11, senators introduced the Children and Teens' Online Privacy Protection Act by updating data privacy rules to protect children and teenagers online. Amending the Children's Online Privacy Protection Act (COPPA), the legislation prohibits internet companies from collecting personal information from anyone 13- to 15-years old without the user's consent. It also requires companies to permit users to eliminate personal information from a child or teen and limits the collection of personal information from teens. The bill further establishes a Youth Privacy and Marketing Division at the FTC to address marketing directed at children and minors, and to question their privacy.

U.S. LITIGATION AND ENFORCEMENT

- **Illinois Supreme Court Affirmed Duty to Defend Decision in BIPA Suit.** In a 6-1 decision, the Illinois Supreme Court affirmed entry of summary judgment in favor of the plaintiff in a duty to defend an insurance coverage lawsuit. In the underlying lawsuit, Krishna, an L.A. Tan franchisee, was accused of violating Biometric Information Privacy Act (BIPA) by, among other things, collecting, using, storing, and disclosing customers' fingerprints without obtaining a written release. The questions for the Court aimed to determine if the underlying allegations: (i) constituted a personal injury "arising out of … oral or written publication of material that violates a person's right of privacy," as required for coverage under the tanning salon's insurance policy; and/or (ii) fell within the insurance policy's so-called violation of statutes exclusion, which excludes coverage for violations of "[a]ny statute, ordinance or regulation … that prohibits or limits the sending, transmitting, communication or distribution of material or information." Affirming the Appellate Court of Illinois, First District, the Illinois Supreme Court found that the BIPA allegations fell within the policy's definition of personal injury and that the violation of statutes exclusion did not bar coverage. Accordingly, West Bend has a duty to defend Krishna in the underlying BIPA suit.

- **Everalbum Facial Recognition Settlement Finalized with the FTC.** On May 7, the FTC finalized a settlement with Everalbum, a California-based photo app developer, involving allegations that it was using its consumers' photos and videos to create facial recognition technology without their express consent. The finalized settlement requires the developer to "obtain consumers' express consent before using facial recognition technology on their photos and videos, [and requires the developer to] delete photos and videos of [] users who deactivated their accounts and the models and algorithms it developed by using the photos and videos uploaded by its users." To read more about the settlement and to learn more about facial recognition software, click here.

- **Demonstrating Increased Risk of Future Harm Trickier in Second Circuit.** In its first decision addressing Article III standing for data breach class actions, *McMorris v. Carlos Lopez & Assocs. LLC*, No. 19-4310, 2021 U.S. App. LEXIS 12328 (2d Cir. Apr. 26, 2021), the Second Circuit Court of Appeals endorsed a nonexclusive three-factor framework for determining whether plaintiffs alleging an increased risk of future identity theft or fraud can establish standing. In *McMorris*, plaintiffs were current and former employees of Carlos Lopez & Associates (CLA), an employer that had inadvertently mailed a spreadsheet containing plaintiffs' PII to all other current CLA employees. In affirming dismissal of plaintiffs' class action for lack of standing, the court found insufficient evidence of "increased risk" of future fraud or identity theft. However, the court left open the

possibility that standing could still be established where plaintiffs allege a sufficient likelihood of misuse of their personal data — especially if the data in question is particularly sensitive and/or was exposed through the efforts of a malicious third party. You can read more about this case here.

- **NY AG Settles with Water Filtration LLC over Data Breach.** Online water filtration provider Filters Fast Co. agreed to resolve an investigation by the New York Attorney General's Office into a 2019 data breach the company failed to disclose that exposed PII for approximately 320,000 U.S.-based customers. In addition to paying $200,000, the retailer will create new incidence response protocols and allow third-party cybersecurity assessment for the next five years. Cybercriminals caused the incident by exploiting a known software vulnerability in the retailer's online checkout process, and the company first began notifying consumers over a year after the initial intrusion.

INTERNATIONAL REGULATION AND ENFORCEMENT

- **Belgian DPA Approves EU Data Protection Code of Conduct for Cloud Service Providers.** On May 20, nearly a decade after former European Commission Vice President Neelie Kroes pitched plans for an EU Code of Conduct for cloud services, the Belgian Data Protection Authority (DPA), serving as the lead authority behind the initiative, announced that it had approved the EU Data Protection Code of Conduct for Cloud Service Providers (the EU Cloud Code of Conduct), the first transnational EU code of conduct since the EU General Data Protection Regulation (the GDPR). With its passage, cloud service providers now have a baseline for implementation and practical guidance for demonstrating compliance with Article 28 of the GDPR. As part of the approval process, the European Protection Board provided a favorable opinion regarding the Cloud Code of Conduct. In addition, the Belgian DPA also accredited Scope Europe as the required monitoring body for the EU Cloud Code of Conduct.

- **Germany Passes Telecom Privacy Law.** On May 20, the German Parliament passed new data protection and privacy laws to synthesize conflicting provisions in existing law and to sync Germany's laws with the GDPR. The Datenschutzes und der Privatsphäre in Telekommunikation und Telemedien (TTDSG) unifies Germany's Telemedia (TMG) and Telecommunications (TKG) acts and implements requirements such as requiring users to agree to cookie settings — a provision already required by EU law since 2009. Opponents of the legislation claim the TTDSG is a "smokescreen," and does not go far enough to protect privacy. TTDSG also attempts to increase high-speed fiber optic internet access for Germans who currently lag far beyond most of Europe at a coverage rate of only 4.7%. Parliament's efforts may all be for naught however, as the TTDSG was passed while the EU continues to hold intense talks on ePrivacy Regulation that could have major ramifications for data protection across all of Europe.

- **Facebook Ireland Can't Shake Irish DPC's Inquiry into International Data Transfers.** Ireland's High Court dismissed an attempt by Facebook to force Ireland's Data Protection Commission (DPC) from ending its inquiry into Facebook's data transfer policies. The inquiry, which centers around the use of standard contract provisions to send user data internationally, is likely to severely restrict Facebook's flow of user information from the EU to the U.S. The ruling initially dismissed the DPC's arguments that its inquiry was not subject to judicial review, but still found that Facebook's challenges to DPC's investigatory procedures did not entitle Facebook to relief. DPC's inquiry will almost assuredly have a huge impact on other large tech firms as well by

forcing companies to keep user data in the EU and process it according to EU standards.

TROUTMAN PEPPER TEAM SPOTLIGHT: MOLLY DIRAGO

Molly is a partner in Troutman's Chicago office. She litigates complex business matters, focusing on privacy, data security, and class actions. As a member of the firm's Privacy and Technology group, Molly also counsels clients on privacy policies, including on the collection of biometric data (fingerprints, retina scans, etc.), and has written articles and spoken on privacy and technology issues, including Illinois' Biometric Information Privacy Act (BIPA). She is a Vice-Chair of the Cybersecurity and Data Privacy committee of the ABA's Tort, Trial & Insurance Practice section.

Molly also enjoys contributing to the legal community through pro bono and public service efforts. She is a passionate advocate for diversity, equity, and inclusion in both legal and business communities and focuses her community service on organizations working toward those goals. She is a board member of the Chicago chapter of the National Organization for Women (NOW), a junior board member of the Women in Law Empowerment Forum (WILEF), and a delegate for the Coalition of Women's Initiatives in Law. She has also written articles for Illinois Legal Aid Online and holds a position with the parent teacher organization (PTO) for her children's school.

Molly dedicates her time to internal efforts to promote diversity as the chair of her office Recruiting Committee and as a member of Troutman's Women's Leadership Committee. In her free time, Molly forgets everything she was taught about legal writing and works on her creative writing, having won contests and publication for her short stories. She is an associate editor of the Chicago Writers Association's literary magazine, *the Write City Review*. She lives in Chicago with her husband, two kids, and a (slightly crazy) cat.

WEBINARS

- On June 24, from 1:00pm to 5:00pm Central Time, the FTC and its regional partners in Dallas will host a free, virtual workshop to discuss advertising and data security basics for advertising professionals, small businesses, and attorneys who advise them. Bringing together national and state legal experts with Texas business owners, marketing executives, and attorneys, the *Green Lights & Red Flags: FTC Rules of the Road for Businesses* workshop will provide insights about the application of consumer protection principles in today's fast-paced marketplace. Acting FTC Chairwoman Rebecca Kelly Slaughter will open the workshop and discussion topics include social media marketing, children's online privacy, email marketing, data security basics, and ethics issues for attorneys. The full agenda is available on the event page. A full agenda and registration are available on the event page.

RECENT TROUTMAN PEPPER PUBLICATIONS

- Facing Up to Tough Issues: Health Care Compliance Concerns with Facial Recognition Technology
- Second Circuit Clarifies Article III Standing Threshold for Data Breach Class Actions
- Eleventh Circuit Throws Debt Collectors Under the FDCPA Bus for Sharing Account Information with Letter Vendors

- Display of Data Symbols Similar to QR Code Visible Through Envelope Window Insufficient to Establish Article III Standing
- Possible Increase in Federal and State Data Privacy Enforcement Actions in 2021
- Google Says “Yes” to More Privacy Requirements

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management