Articles + Publications | August 2022

More Privacy, Please – August 2022

WRITTEN BY

Molly S. DiRago | Kim Phan | Connor DeFilippis | Ronald Raether, Jr. | James Koenig | Robyn W. Lin | Alexandria Pritchett

Authors:

Molly DiRago
Kim Phan
Robyn Lin
Connor DeFilippis
Alexandria Pritchett
Ron Raether
Jim Koenig

Lisa Amador*
Safvet Besen*
Phoebe Cooper*
Chloe Lee*
Jovanni Villa*

Editor's Note: In the U.S. laws and regulation space, federal lawmakers continued to push the American Data Privacy and Protection Act forward, and the FTC pledged to enforce the law against the illegal use of highly sensitive data, including health data. Meanwhile, the California Privacy Protection Agency commenced official rulemaking. In U.S. litigation, courts continued to see BIPA litigation, including a claim against an educational institution and a claim against Clearview AI. In international regulation and enforcement, the European Parliament passed the Digital Marketing Act and the Digital Services Act, and the U.K. introduced a new post-Brexit data privacy bill. Elsewhere, Ireland sought to halt Meta's transfer of data from Ireland to the U.S., and Iceland fined the city of Reykjavik for processing children's data.

US Laws and Regulation

- **House Committee Amends American Data Privacy and Protection Act.** On July 19, the House Committee on Energy and Commerce approved an amendment as a substitute to the current American Data Privacy and Protection Act draft. The amendment makes several notable changes, including changing the private right of action's effective date from four years to two years post-adoption, providing the California Privacy Protection Agency with enforcement power, and adding technical changes to the "covered entity" and "service provider" definitions. To view the amendment, click here.

- **FTC Pledges Law Enforcement Against Illegal Use and Sharing of Highly Sensitive Data.** In a July 11 blog post, the Federal Trade Commission (FTC) committed to fully enforcing the law against illegal use and sharing of highly sensitive data. The FTC referenced the FTC Act Section 5, which prohibits unfair or deceptive acts or practices, the GLBA Safeguards Rule, the HIPAA Health Breach Notification Rule, and the Children's Online Privacy Protection (COPPA) Rule. The blog post stated that "[t]he Commission is committed to using the full scope of its legal authorities to protect consumers' privacy. We will vigorously enforce the law if we uncover illegal conduct that exploits Americans' location, health, or other sensitive data. The FTC's past enforcement

©2026 Troutman Pepper Locke

actions provide a roadmap for firms seeking to comply with the law."

- **DOJ Investigates Federal Court Records System.** On July 28, the Department of Justice (DOJ) announced it was investigating a cyber breach involving the federal court records management system. Matt Olsen, head of DOJ's National Security Division, told the House of Representatives Judiciary Committee that the incident was a "significant concern." Olsen said the DOJ was working closely with the federal judiciary around the country to address the issue. He did not comment on who originated the attack.

- **National Credit Union Administration May Require Credit Unions to Report Cyber Incidents.** On July 26, the National Credit Union Administration announced a proposed rule to require federally insured credit unions experiencing a reportable cyber incident to report the incident to the agency as soon as possible and no later than 72 hours after the credit union reasonably believes it experienced a reportable cyber incident. This proposed rule would not require a detailed incident assessment, but just an early alert to the agency. Comments to the proposed rule are due on or before September 26.

- **Senators Introduce Improving Digital Identity Act.** On July 21, U.S. Senators Krysten Sinema (D-AZ) and Cynthia Lummis (R-WY) introduced the Improving Digital Identity Act of 2022. The legislation would create a taskforce to improve cybersecurity to allow access to "critical services" online. It also would require federal agencies to strengthen the "security, accessibility, and privacy" of their networks.

- **Two Children's Privacy Bills Advance to Senate.** On July 27, the U.S. Senate Committee on Commerce, Science, and Transportation advanced two federal bills to protect children and teenagers' online privacy. S1628 would update COPPA, including extending the law's applicability to children through age 17, while S3663 would update the Kids Online Safety Act.

- **CPPA Begins Formal Rulemaking.** On July 8, the California Privacy Protection Agency (CPPA) commenced the formal rulemaking process to adopt the first set of regulations to implement the Consumer Privacy Rights Act of 2020. To participate in the public portion of the rulemaking process, interested parties may submit written comments by August 23.

US Litigation and Enforcement

- **American Airlines Unit Reaches BIPA Settlement Over Fingerprint Collection Concerns.** On July 7, Envoy Air — a unit of American Airlines — settled claims by a former customer service agent that the airliner violated provisions of the Illinois Biometric Information Privacy Act (BIPA). Brought as a putative class action, the suit alleged among other things that Envoy failed to provide adequate information or obtain proper consent as to how it collected, used, and maintained employees' fingerprint scans as required by employees to clock into shifts. Envoy moved to dismiss the complaint in early 2021. The court partly granted this motion, dismissing the plaintiff's BIPA claims as they related to conduct after June 2016 when labor negotiations began that ultimately led to controlling grievance procedures. The parties informed the court in July that they reached a settlement agreement.

- **FACTA Class-Action Dismissal Affirmed for Lack of Standing.** A plaintiff's lack of standing proved fatal to

his Fair and Accurate Credit Transaction Act (FACTA) class action on July 13 when a Florida appeals court affirmed the suit's dismissal. The plaintiff alleged that Red Wing Shoe Co. violated FACTA when it provided him a receipt that showed 10 digits of his credit card number. FACTA prohibits the printing of more than the last five digits of a credit or debit card's number on a receipt. The trial court dismissed the complaint, finding that the plaintiff had not alleged any resulting or possible harm based on the statutory violation. Indeed, the plaintiff retained the receipt during the entire litigation. Accordingly, there was no injury in fact that provided the plaintiff with the requisite standing. The appeals court affirmed, finding that a concrete injury was required, and the plaintiff could not sue for statutory damages under FACTA for a mere violation without resulting harm.

- **Illinois Institute of Technology Subject to BIPA.** On July 18, U.S. district judge for the Northern District of Illinois decided that the Illinois Institute of Technology (IIT) must face allegations that the Chicago-based research university violated BIPA by requiring students to use an online proctoring tool that used facial recognition technology to verify their identity without their permission. The judge agreed that the school could be deemed a "financial institution" protected by the Gramm-Leach-Bliley Act, which would exempt the institution from BIPA's informed consent requirements, but noted it was too early to tell if IIT qualifies for the exemption, stating: "[T]he fact that IIT is a participant in federal student aid programs does not, by itself, establish that IIT is regularly extending or administering student loans." Whether IIT falls into that category "presents a question of fact better addressed at a later stage in the proceedings."

- **Lawsuit Filed Against Clearview AI Over Biometric Privacy.** On July 7, Illinois, California, and New York residents filed an amended complaint in the U.S. District Court for the Northern District of Illinois against Clearview AI to include additional client defendants, such as AT&T and Walmart. The complaint alleges that Clearview collected facial images from the internet without obtaining consent to create a database that Clearview's clients could use to identify individuals from their biometric information. The plaintiffs argue that this violates BIPA and other state constitutional, statutory, and common law. Additionally, the plaintiffs seek relief from the "Clearview Client Class," which includes nongovernmental and private entities with access to Clearview's facial recognition database. The court permitted eight claims from the original pleading to proceed.

International Regulation and Enforcement

- **New EU Digital Rulebook Provides Standard for Accountability.** On July 5, the European Parliament voted in favor of the new Digital Services Act (DSA) and Digital Markets Act (DMA). The two bills address the societal and economic effects of the tech industry by setting clear standards for operation and provision of services in the EU. The DSA establishes obligations for digital service providers, such as social media or marketplaces, to tackle the spread of illegal content, online disinformation, and other societal risks. In other words, what is illegal offline, should be illegal online. These obligations intend to be proportionate to the size and risks that such platforms pose to society. Accordingly, large platforms with 45 million or more monthly users will have to comply with stricter obligations as they present the highest risk.

- **UK Introduces New Data Reform Bill.** On July 18, the U.K. government introduced a post-Brexit data reform initiative to help guide responsible use of data, while promoting innovation. The Data Protection and Digital Information Bill contains six parts: data protection, digital verification services, customer data and business data, other provisions about digital information, regulation and oversight, and final provisions. The bill also includes a

section on automated decision-making. Separately, the U.K. government proposed a second set of rules and regulations for AI and machine learning, intending to complement the data protection bill.

- **Iceland DPA Fines Capital City of Reykjavik for Processing Children's Data.** Iceland's data protection authority (DPA), Persónuvernd, fined the city of Reykjavík 5 million kronor ($36.7 thousand USD) over data processing in the Seesaw student system used in primary schools. The DPA said the violations "concerned the personal data of children who enjoy special protection under the Data Protection Act and that it was considered likely that their sensitive personal data and information was entered as teacher feedback and information on students' private affairs." The DPA noted that the purpose for processing was not clearly defined, and data minimization principles were not followed. Additionally, there was insufficient authorization for the data processing, as well as a "high risk" of transferring data to the United States without proper safeguards. However, the DPA also acknowledged that no damage occurred from the breaches, Seesaw's overall information security was satisfactory, and the city of Reykjavik responded to the DPA in a clear and timely manner and stopped further processing without parental approval.

- **Irish DPC Seeks to Halt Meta's Data Transfers to the US.** On July 7, Ireland's Data Protection Commission (DPC) sent a draft decision to its EU DPA counterparts in which it proposed to halt Meta from transferring users' personal data from the EU to the United States. If approved by other DPAs, Meta-owned services like Facebook and Instagram could be heavily impacted in the EU. Ireland's DPC inquiry follows the Court of Justice of the European Union's (CJEU) decision that invalidated the EU-U.S. Privacy Shield Framework. After the Privacy Shield Framework's invalidation, many companies like Meta have relied on standard contractual clauses (SCCs) to complete their data transfers. The Irish DPC's draft decision could mean that these companies can no longer rely on SCCs to transfer data to the United States. The proposal will have no immediate effect on Meta's services or practices, but under Article 60 of the EU General Data Protection Regulation, other DPAs will have four weeks to comment or express "relevant or reasoned objections" to the DPC's draft, but ultimately, a final decision could take longer than four weeks.

- **TikTok Pauses Update in Response to Irish DPC.** On July 12, TikTok paused a controversial European privacy policy update due to widespread privacy concerns, including an analysis implemented by the Irish DPC. If implemented, the advertising update would allow TikTok to stop asking users for their consent to be tracked. Italy's DPA also issued a formal warning to TikTok, stating that TikTok's plan to switch from asking users for their consent to run "personalized" ads to processing behavioral advertising data based on "legitimate interest," which would not require a user's prior consent, would breach the ePrivacy Directive. The ePrivacy Directive requires companies to obtain a user's consent before storing cookies on a user's browsers, except for strictly necessary cookies.

Troutman Pepper Team Spotlight: Alison Grounds

As a highly skilled eDiscovery advocate, Alison leverages legal strategy and technology to discover the facts needed to help clients win cases, settle at the right value, resolve internal investigations, comply with

governmental requests, and assist with breach response requirements. Known for her proactive, practical, efficiency-obsessed approach to discovery, Alison also uses her prior trial experience to inform her discovery advocacy. As such she has successfully argued on behalf of clients to both remediate and avoid sanctions for discovery conduct occurring before her engagement and to achieve case-terminating sanctions and fees against adversaries failing to comply with their discovery obligations.

Recognizing that most of the increased costs and risks of the discovery process come from too many disconnected stakeholders and processes, Alison founded and leads eMerge — the firm's wholly owned subsidiary focused on providing clients with end-to-end, integrated discovery services. eMerge's attorneys and technologists combine legal strategy, advanced technology, and project management to manage data in legal matters. Alison also advises clients on litigation readiness and data management issues.

Alison serves an adjunct professor of eDiscovery and legal technology at Emory University School of Law, frequently speaks and authors publications on eDiscovery issues, and ranks high in *Chambers and Partners*. She also serves on the firm's policy, partner compensation, innovation, and information technology committees.

As strong advocates for dog/cat rescue, Alison and her partner Ashley have fostered over 120 dogs and encourage others to "adopt don't shop." They named their latest rescue "Ricki Baker" after the foster kid in the movie *Hunt for the Wilderpeople*.

Upcoming Events

- Ron Raether (Speaker), "Testing Screening Operations for Potential Unintended Discrimination," PBSA, September 12, 2022.
- Sadia Mirza (Speaker), "Mother Knows Best – Fireside Chat w/the Moms Leading Privacy, Risk & Security," IAPP P.S.R., October 13-14, Austin, TX.
- Ron Raether (Speaker), "Financial Privacy, Data and Security," 12th Annual National Institute on Consumer Financial Services, October 20, 2022.

**2022 summer associates with Troutman Pepper and not licensed to practice law in any jurisdiction.*

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management