Articles + Publications | July 2022

More Privacy, Please – July 2022

WRITTEN BY

Molly S. DiRago | Ronald I. Raether Jr. | Rachel Buck Hodges | Connor DeFilippis | Kim Phan | James Koenig | Matthew R. Cali | Alexandria Pritchett | Robyn W. Lin

Authors:

Molly DiRago
Kim Phan
Robyn Lin
Connor DeFilippis
Matthew Cali
Rachel Buck
Alexandria Pritchett
Ron Raether
Jim Koenig
Zach Cimring*
Taylor Henderson*
Phoebe Cooper*
Ben Duwve*
Justin Stalberg*
Safvet Besen*

Editor's Note: In the U.S. laws and regulation space, federal lawmakers formally introduced bipartisan comprehensive federal privacy legislation titled, the American Data Privacy and Protection Act. Meanwhile, California passed a bill intended to protect children's online privacy, and the California Privacy Protection Agency approved draft regulations. The FTC republished an advance notice of proposed rulemaking on artificial intelligence and algorithms, and a new trans-Atlantic framework was announced between the United States and the European Union. In U.S. litigation, Microsoft and Walmart will face BIPA claims in Illinois, and several district courts approved settlements over data breaches. In international regulation and enforcement, Canada introduced a new comprehensive federal data privacy law, just as its beloved coffee chain comes under scrutiny for tracking customers' locations. Also, European authorities published five fairness guidelines for children's advertising, and the U.K. government published a response concerning data protection reform.

US Laws and Regulation

- **Lawmakers Introduce Federal Privacy Legislation.** On June 21, lawmakers formally introduced H.R. 8152, a comprehensive federal privacy legislation titled, the American Data Privacy and Protection Act (ADPPA). The bipartisan bill would provide a private right of action when a "substantial privacy harm" occurs and would largely preempt state laws with some exemptions. The ADPPA underwent a mark-up session on June 23 and was voted out of the committee. For a draft of the bill, click here, and to learn more about this topic, listen to Kim Phan's CDIA July 6 webinar "To Be or Not to Be? Bipartisan U.S. Federal Privacy Bill Gains Momentum" by registering here.

- **President Biden Signs the State and Local Government Cybersecurity Act of 2021.** On June 21, President Biden signed the State and Local Government Cybersecurity Act of 2021 (S.2520), which updates the Homeland Security Act and directs the Department of Homeland Security to improve information sharing and

coordination with state, local, and tribal governments. This legislation encourages federal cybersecurity experts to share information on cybersecurity threats, vulnerabilities, and breaches, as well as resources to prevent and recover from cyberattacks. The law also builds on previous efforts by the Multi-State Information Sharing and Analysis Center (MS-ISAC) to prevent, protect, and respond to future cybersecurity incidents. For more information, click here.

- **Democratic Senators Introduce Health and Location Data Protection Act.** On June 15, Senators Elizabeth Warren (D-MA), Ron Wyden (D-OR), Patty Murray (D-WA), Sheldon Whitehouse (D-RI), and Bernie Sanders (I-VT) introduced the Health and Location Data Protection Act, which would ban data brokers from selling health and location data. The act empowers the Federal Trade Commission (FTC), state attorneys general, and injured persons to sue to enforce the law, while also providing $1 billion in funding to the FTC. For more information, click here.

- **MD Student Privacy Act Takes Effect June 1.** Maryland Senate Bill 325 took effect on June 1, expanding the protection of K-12 students' data, modifying the scope of covered information, and further restricting what data can be used in targeted advertising. The law also creates a Student Data Privacy Council to study the impacts of the law and make recommendations regarding best practices for ensuring compliance. Finally, the law requires the council to submit a report to the governor and legislature, assessing the law's effectiveness and providing recommendations for statutory changes before December 1, 2025.

- **California Age-Appropriate Design Code Act Passes State Assembly.** On May 26, the California State Assembly passed Assembly Bill 2273, concerning online privacy protection for children. Enforceable by the California Privacy Protection Agency (CPPA), the act adds provisions protecting children's online data and online exposure for individuals under the age of 18. The bill awaits Senate consideration before August 31 (the final day to pass bills in either legislative chamber), and if passed in both chambers, the governor must veto or sign the bill before September 30.

- **California Privacy Protection Agency Approves Draft Regulations.** On June 8, the California Privacy Protection Agency Board voted unanimously to authorize Executive Director Ashkan Soltani to begin the California Privacy Rights Act (CPRA) rulemaking process. Previously, the agency released draft regulations to prepare for the June 8 meeting, and it will now file a Notice of Proposed Rulemaking Action to begin the formal rulemaking process.

- **FTC Refiles ANPRM on Privacy and AI Algorithms.** Originally slated for last February, on June 1, the FTC refiled an Advanced Notice of Proposed Rulemaking (ANPRM) with the Office of Management and Budget for a potential rule on artificial intelligence and privacy abuses under Section 18 of the FTC Act. Stakeholder consultation began June 1 and will end August 1. The FTC hopes to curb lax security practices and combat unlawful discrimination in algorithm decision-making. Click here to view the ANPRM.

- **FTC Seeks Input on Modernizing Business Guidance.** On June 3, the FTC announced its request for input on ways to modernize the agency's business guidance: ".com Disclosures: How to Make Effective Disclosures in Digital Advertising." First published in March 2013, the FTC seeks guidance on several issues, including the use of sponsored and promoted advertising on social media, the adequacy of online disclosures when consumers must navigate multiple webpages, and whether the current guidance adequately addresses

advertising on mobile devices. To read the announcement, click here.

- **DOJ Reaches Settlement in Meta Advertising Discrimination Case.** On June 21, the U.S. Department of Justice reached a settlement (to be approved by the Southern District of New York) in a case against Meta Platforms, Inc., (formerly Facebook, Inc.), alleging that Meta's housing advertisements on various social media platforms, including Facebook, Instagram, and Messenger, violated the Fair Housing Act. More specifically, Meta's advertisement algorithms allegedly discriminated against Facebook users on the basis of their race, religion, sexual orientation, familial status, disability, and national origin. According to the settlement agreement, Meta must: (1) stop using its current algorithm, (2) create a new algorithm that does not discriminate; (3) subject to monitoring by an independent organization, as well as the U.S. to ensure its compliance with anti-discrimination standards; (4) notify authorities upon any intention to add targeting options for housing advertisements; (5) provide regular compliance reports; and (6) pay $115,054, the maximum penalty for violations of the Fair Housing Act.

- **GAO Warns Action Is Needed to Assess the Potential Federal Response to Catastrophic Cyberattacks.** A new report from the U.S. Government Accountability Office (GAO) warned about an increased risk in cyberattacks and recommended the federal government undertake certain studies to assess the impact of such attacks and how it will respond. The report cautioned that cyberattacks threaten "catastrophic" harm to the country's utilities, financial systems, and energy pipelines, which will "spill over from the initial target to economically linked firms — magnifying damage to the economy." The full GAO report may be found here.

- **HHS Guides Telehealth Services on HIPAA Compliance.** On June 13, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) released guidance on how health care providers and health plans can use remote communication technologies to provide audio-only telehealth services that comply with the Health Information Portability and Accountability Act (HIPAA) privacy, security, and breach notification rules. OCR Director Lisa J. Pino stated that audio-only telehealth can assist "in reaching patients in rural communities, individuals with disabilities, and other seeking the convenience of remote options." To read more, click here.

US Litigation and Enforcement

- **OPM Hack Plaintiffs Win Initial Approval for $63M Settlement.** On June 8, U.S. District Judge Amy Berman Jackson gave preliminary approval for the $63 million settlement in a class action brought by the victims of the 2015 Office of Personnel Management (OPM) data breach. The settlement, which would provide awards between $700 and $10,000 to eligible persons, resolves the long-running legal claims that have gradually filtered through the U.S. courts in the wake of the June 2015 incident, affecting over 25.7 million current and former federal employees. While it was unclear who orchestrated the attack, experts agree the cyberattack was carried out on behalf of foreign governments. Under the proposed settlement, OPM will pay $60 million into the settlement, and Peraton, a contractor that operated the electronic information systems, will contribute $3 million.

- **TX Drivers Ask SCOTUS to Resolve DPPA Circuit Split.** On June 8, a class of Texas drivers asked the U.S. Supreme Court to decide whether the Driver's Privacy Protection Act (DPPA) covers information that is available, but not directly disclosed to the public. The class, which arose in the Fifth Circuit, alleges that

Vertafore, Inc.'s storage of drivers' private information on a publicly accessible server violated the DPPA. In 2015, the Seventh Circuit ruled that a public disclosure of private information through a parking ticket on a windshield violated the DPPA, but in this case, the Fifth Circuit held that storage of private information on an unsecured server did not create a disclosure violating the DPPA.

- **Accellion to Pay $8.1M Settlement Over 2020 Data Breach.** On June 16, the plaintiffs who brought a class action against Accellion filed a motion for preliminary approval of a settlement for $8.1 million in the Northern District of California. If approved, class members would receive two of three credit monitoring and insuring services, reimbursement of up to $10,000, or a cash fund payment between $15 and $50. The settlement also would provide injunctive relief to be implemented four years from the effective date of the settlement. This will require Accellion to retire its file-sharing product "File Transfer Appliance," provide annual cybersecurity training to all employees, employ personnel with formal cybersecurity responsibilities, and take other measures. The settlement stems from a late 2020 data breach where hackers stole names, dates of birth, Social Security numbers, drivers' license numbers, and bank account information from law firms, universities, and government agencies.

- **Dollar Bank Faces $4.3M Negligence Lawsuit Over Fraudulent Transfers.** On June 1, a Pennsylvania Court of Common Pleas denied a Pittsburgh-based bank's motion to dismiss negligence claims filed by one of its customers. The customer, a 79-year-old woman from suburban Pittsburgh, was duped by phone scammers into transferring $4.3 million into a cryptocurrency account, with local Dollar Bank employees assisting the customer with these transactions. In response to the lawsuit, the bank argued that it followed the rules of Uniform Commercial Code Article 4A, dealing with wire transfers, and otherwise had no reason to know the fraudulent nature of the transfers. The customer argued that she did not challenge the transfers themselves, but instead claimed that the bank failed to follow its own policies to protect customers and stop suspicious transactions.

- **$6M Class-Action Settlement for BIPA Fingerprint Scan Violations Approved.** BioLife Plasma and a class of over 26,000 plasma donors inked an agreement to settle claims that the plasma company failed to follow Biometric Information Privacy Act (BIPA) disclosure and consent requirements when obtaining fingerprint scans. On June 6, a Cook County judge approved the settlement, which after fees, costs, and awards for the class representatives, will net claimants about $3.75 million. Claimants who had their fingerprints scanned before March 6, 2020 will take home the lion's share of the settlement since BioLife updated its allegedly deficient consent forms that month. Post-March 6 claimants will still see some of the settlement since class counsel argued that BioLife still failed to comply with BIPA by not posting its consent forms online.

- **Microsoft Faces Class-Action BIPA Lawsuit Over Azure Payroll System.** On May 26, plaintiff Natasha Jones filed a class-action lawsuit against Microsoft for violating the Illinois BIPA. The complaint alleges that Microsoft improperly held workers' fingerprints — sensitive biometric identifiers — on the Azure payroll system without obtaining written consent and failed to make its biometric information retention policies clear. Jones' complaint also alleges that by holding the workers' fingerprints on Azure, Microsoft profited from its BIPA violations through its clients' payments to use Azure.

- **Walmart Sued Under BIPA for Use of Voice Tracking Software.** On May 31, A Northern District of Illinois judge dismissed Walmart's motion to dismiss a class action, alleging Walmart violated BIPA by requiring warehouse workers to speak into a headset with software that captured and used their voiceprints without their

consent. The court denied the motion to dismiss because the ultimate question — Can the retailer's headset software identify individuals? — "is a factual question that is better addressed after discovery." Walmart argued that the plaintiff failed to allege that the voice recording system collected biometric data because the system could not identify specific employees by their voice.

International Regulation and Enforcement

- **Canada Introduces Federal Comprehensive Privacy Act.** On June 16, the Canadian Minister of Innovation, Science, and Industry introduced the Digital Charter Implementation Act 2022, which features three pieces of legislation: the Consumer Privacy Protection Act (CPPA), the Personal Information and Data Protection Tribunal Act, and the Artificial Intelligence and Data Act. The CPPA would replace the current privacy framework — the Personal Information Protection and Electronic Documents Act (PIPEDA) — and would provide consumers greater control over their personal information. The second component would establish a tribunal to oversee CPPA violations, and the third legislation would require companies that build high-impact artificial intelligence systems to identify, assess, and mitigate the risk of harms and bias.

- **Popular Canadian Coffee Chain Under Scrutiny.** On June 1, the Office of the Privacy Commissioner of Canada (OPC) announced the result of a joint investigation with the Commission d'accès à l'information du Québec, the Office of the Information and Privacy Commissioner for British Columbia, and the Office of the Information and Privacy Commissioner of Alberta into popular Canadian coffee chain Tim Hortons. The investigation found that the Tim Hortons app collected 'vast amounts' of sensitive location data about individuals and tracked their movements every few minutes of the day. This information was collected even when users were not in the app so long as the device was on. Tim Hortons agreed to comply with the agencies' recommendations, including deleting any remaining location data and establishing a privacy management program.

- **Vinted AUB Investigation Signals Cooperation Among Data Protection Supervisory Authorities.** On June 2, a working group of French, Lithuanian, and Polish supervising authorities (SAs) began examining a series of complaints concerning potential compliance infringements of clothing retailer Vinted UAB. SAs plan to investigate issues concerning transparent information and storage of data on the withdrawal of funds after the online clothing sales website — vinted.com — received a significant number of complaints. The data protection authorities said that the SAs involvement demonstrates close cooperation between SAs in law enforcement, an essential strategy for the European Data Protection Board (EDPB). If successful, the EDPB intends to use this form of collaboration more frequently in the future.

- **European Authorities Publish Fairness Principles for Children's Advertising.** Recognizing that children are particularly susceptible to "problematic" marketing practices, European consumer and data protection authorities developed five fairness principles for advertising directed at children. Published on June 9, the fairness principles are: (1) accounting for the specific vulnerabilities of children, (2) not exploiting children's age or credulity, (3) identifying advertising content in a manner that is clear and age appropriate, (4) not prompting in-app purchases in content marketed as "free," and (5) not profiling children for advertisement purposes. These principles are directed toward businesses to help them avoid harmful advertising practices and better educate consumers about such practices. While not legal requirements, the principles intend to supplement European

consumer and data protection legislation like the GDPR and Unfair Commercial Practices Directive.

- **UK Government Publishes Response on UK Data Protection Law.** On June 17, the Department for Digital, Culture, Media, and Sport (DCMS) published its response to proposals collected on U.K. data protection law. The response sets out 63 reform proposals that the government intends to take. Moving forward, DCMS will focus on five key areas: (1) reducing barriers to responsible innovation; (2) reducing burdens on business and delivering better outcomes for people; (3) boosting trade and reducing barriers to data flows (4) delivering better public services; and (5) reforming the Information Commissioner's Office. The queen's speech in May evidenced the government's intention to introduce a Data Protection Reform Bill, and a draft of the bill is expected soon.

- **Congressional Research Service Update to Trans-Atlantic Data Privacy Framework.** On June 2, The United States and European Union released the Trans-Atlantic Data Privacy Framework (TADP). The TADP details the U.S. and EU's plan to protect data and ensure trans-Atlantic trade across the regions. The TADP mandates companies to follow the privacy shield principles and "self-certify through the U.S. Department of Commerce." The framework has seven principles, including "notice; choice; accountability for onward data transfer; security; data integrity and purpose limitation; access; and recourse, enforcement, and liability." The U.S. Department of Commerce, U.S. Federal Trade Commission, U.S. Department of Transportation, and European Commission will enforce the framework, which they hope to implement by the end of the year.

Troutman Pepper Team Spotlight: Josh Davey

Josh has experience in data breach and cybersecurity litigation, and he serves as one of the court-appointed lead defense counsel for a large cloud software company in multidistrict litigation proceedings. He represents banks, mortgage companies, auto and credit card lenders, and other financial services industry clients facing high-risk consumer class actions, government investigations, or business disputes. He has a long and proven track record of achieving favorable outcomes in these matters, working with clients to identify the resolution that will best meet their business needs. He routinely handles significant litigation matters across the country, and has represented clients in governmental investigations and enforcement proceedings involving the Consumer Financial Protection Bureau, the Office of the Comptroller of the Currency, the Department of Justice, and state attorneys general.

In high school, Josh played bass guitar in a band, and his now wife of 22 years played the drums. Today, they have nine children ranging from 2 to 16, and are expecting their 10th in November.

Upcoming Events

- Kim Phan (Speaker), "Data Breach Developments," Real Estate Services Providers Council(RESPRO), July 13, 2022.
- Kim Phan (Speaker), "Data Security: Failure Is Not an Option," Compliance University, Online Lenders Alliance (OLA), July 20, 2022.
- 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.

Recent Troutman Pepper Regulations

- California Privacy Protection Agency Publishes Draft Rules
- Dark Web Monitoring
- Troutman Pepper's Fintech Capabilities and Trending Issues Impacting Fintech Companies

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

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management