

More Privacy, Please – September 2022

WRITTEN BY

Jim Calvert | Molly S. DiRago | Ronald I. Raether Jr. | Edgar Vargas | Connor DeFilippis | Kim Phan | Jason Lichter | Robyn W. Lin

Editor's Note: In the U.S. laws and regulation space, the California attorney general announced the first-ever CCPA settlement, the California Privacy Protection Agency raised objections to the ADPPA, and the FTC announced advance notice of a proposed rulemaking aimed at commercial surveillance and data security. Meanwhile, the California legislature passed the Age-Appropriate Design Code Act. In U.S. litigation, Meta settled a class action over tracking and requested attorneys' fees in a data scraping suit. In international regulation and enforcement, Europe's top court provided a ruling on sensitive data, and Norway requested fines for Facebook's alleged illegal transfer of data.

US Laws and Regulation

- **California AG Issues First-Ever CCPA Settlement.** On August 24, California Attorney General Rob Bonta announced a settlement with Sephora for \$1.2 million. AG Bonta alleged that Sephora (1) failed to disclose that it sells data; (2) engaged in the unlawful sale of personal information, including exchanging data with third parties for analytics information; (3) failed to post a "Do Not Sell My Personal Information" link on its website and homepage; and (4) failed to respond to or process consumer opt-outs in accordance with global privacy controls. AG Bonta also released information about several other California Consumer Privacy Act (CCPA) enforcement examples regarding notice of alleged noncompliance, addressing adequate privacy policies, notices of financial incentives, and consumer requests procedures. To review important lessons learned from these announcements, check out Troutman Pepper's [analysis](#).
- **CPPA Circulates Letter on ADPPA.** On August 15, the California Privacy Protection Agency (CPPA) [issued](#) a letter against H.R. 8152, the American Data Privacy and Protection Act (ADPPA). As a comprehensive federal privacy bill, the ADPPA would largely preempt state laws and provide a private right of action. In the letter, the CPPA argued the bill would remove important privacy protections and weaken Californians' privacy rights. The letter urged that ADPPA should be a "floor" of federal protections as opposed to preempting state laws.
- **CA Legislature Fails to Extend Employee and B2B Data Exemptions.** On August 31, the California legislature ended its 2022 session without adopting legislation to extend the CCPA employee and business-to-business (B2B) personal information exemptions. Therefore, on January 1, 2023, this data will be subject to the CCPA for the first time. To prepare for compliance, check out Troutman Pepper's checklist [here](#).
- **FTC Announces Advanced Notice of Proposed Rulemaking.** On August 11, the Federal Trade Commission (FTC) [published](#) an advance notice of proposed rulemaking aimed at commercial surveillance and data security. The FTC invites comments on whether it should undertake rulemaking on the ways companies collect,

aggregate, protect, use, analyze, and retain consumer data. The FTC also seeks information on the ways companies transfer, share, sell, or otherwise monetize data using unfair or deceptive methods.

- **California Passes Age-Appropriate Design Code Act.** On August 30, the California legislature passed AB [2273](#), the Age-Appropriate Design Code Act. The bill imposes certain data privacy requirements on businesses that provide services or products that a child will likely access. The bill now awaits Governor Newsom's signature.
- **Banks Face Billions in Fines by Using Messaging Apps That Stymie Regulatory Investigations.** The Securities and Exchange Commission and the Commodity Futures Trading Commission will likely issue fines totaling up to \$2 billion to many of the largest investment banks for violating recordkeeping requirements applicable to broker-dealer firms, swap dealers, and futures commission merchants. [Bloomberg](#) reported that these federal agencies were frustrated by traders' continued use of unapproved messaging apps that promote secrecy (such as WhatsApp's end-to-end encryption) on personal mobile devices to engage in off-the-record communications, thereby flouting banks' regulatory preservation obligations and impeding government investigations.
- **BBB Delivers Warning for Child-Directed Advertising in the Metaverse.** On August 23, the Better Business Bureau (BBB) National Programs' Children's Advertising Review Unit (CARU) [issued](#) a compliance warning on CARU's self-regulatory guidelines for children's advertising. Specific to the Metaverse, CARU warned that advertisers should be particularly cautious about blurring advertising and non-advertising content, and advertising must be easily identifiable as such. CARU also warned that influencer and endorser advertising must be clearly disclosed, manipulative tactics in advertising are prohibited, and advertising must include clear and conspicuous disclosures.

US Litigation and Enforcement

- **Meta Seeks \$2.7M in Fees in Data Scraping Suit.** On August 17, Meta's attorneys [filed](#) a 22-page motion in the Northern District of California, seeking just over \$2.7 million in fees against the defendants in its ongoing data scraping suit *Meta Platforms, Inc. v. BrandTotal Ltd., et al.*, Case No. 3:20-cv-07182. Meta alleged that the defendant BrandTotal scraped data from Meta's platforms without authorization and continued to scrape despite continued warnings from Meta. After Meta partially prevailed at summary judgment on its California's Comprehensive Computer Data Access and Fraud Act claims, it later argued to recover all reasonable attorney's fees incurred in preparing and filing the motion for summary judgment because it was forced to "spend significant time and resources[.]"
- **Meta Settles Class-Action Claims Over Tracking for \$37.5M.** On August 22, Meta and a class of Facebook users [agreed](#) to settle claims that the tech giant violated users' privacy — and the company's own policies — by using location data to target ads. The class consists of Facebook users who had switched off "location services" on their phones, but still had their locations "inferred" by Meta's use of their IP addresses. The settlement resolves two consolidated cases that included four motions to dismiss and over 100,000 pages of document discovery. If approved, the settlement would create a \$37,500,000 common fund to be distributed pro rata to class members. The plaintiffs' motion to approve the settlement is currently pending in the Northern

- **Third Circuit Revives Privacy Suit Against Harriet Carter Gifts.** On [August 16](#), the Third Circuit overturned a lower court's ruling that Harriet Carter and third-party marketing company NaviStone, Inc. were exempt from liability under Pennsylvania's anti-wiretapping law. The plaintiffs alleged that Harriet Carter used a marketing technology company to automatically spy on, and intercept, interactions between the consumer and Harriet Carter's website. The lower court granted summary judgment, holding NaviStone could not have "intercepted" any communications because it was a "party" to those communications. The Third Circuit drew upon caselaw and legislative interpretation to reverse, holding that no exemption exists for someone who is a "direct party" since all parties must consent.
- **Sterling Jewelers Sues for Invasion of Privacy.** On [August 22](#), customers filed a proposed class action in the Central District of California, alleging that Sterling Jewelers invaded their privacy under California's wiretapping statute by secretly logging users' keystrokes when using the online chat function. The plaintiffs then alleged this information was illegally shared with a third-party spyware company that extracted the data for marketing purposes.
- **Third Circuit Rules Breach Victim Has Article III Standing.** On [September 2](#), the Third Circuit held that a former ExecuPharm, Inc. employee had Article III standing in her negligence class action. Plaintiff Jennifer Clemens alleged that the company's negligence led to a data breach, which leaked her private information onto the dark web. The lower court held she had no standing because she had not suffered identity theft or fraud as a result of the leak. The Third Circuit reversed, holding that under Supreme Court caselaw, "sufficient risk" of future harm could confer Article III standing. The Third Circuit found that this risk was met because (i) a well-known hacker group had intentionally gained access and misused her data by placing it on the dark web, and (ii) the "data was also the type of data that could be used to perpetrate identity theft or fraud." This combination of factors raised a sufficient risk of harm to confer standing.

International Regulation and Enforcement

- **Switzerland Adopts Revised Data Protection Act.** On August 31, the Federal Council [adopted](#) the revised Data Protection Act, which includes implementing updated data protection ordinances and data protection certifications. Among other Data Protection Act revisions, controllers no longer need to document why a communication was refused, restricted, or deferred. The revised Data Protection Act will go into effect on September 1, 2023.
- **Irish DPC Issues €405m Fine Against Instagram.** On September 7, the Irish data protection commissioner (DPC) [issued](#) Instagram a record 405 million euro fine for violating children's privacy. The fine arose out of an investigation that Instagram breached children's privacy because the default settings of "business accounts" operated by child users automatically published mobile phone numbers and email addresses. The investigation also focused on a default setting that set children's profiles to "public" that required the user to manually set it to "private."
- **European Counterparts Object to Irish DPC Draft Meta Decision, Including Calling for Additional**

Sanctions. On July 7, Ireland's DPC issued a draft decision to halt Facebook parent Meta's use of standard contractual clauses (SCCs) to legitimize data transfers from the EU to the U.S. — a decision that Meta said would prevent it from offering Facebook and Instagram in Europe. With a final decision expected in several months, the Irish DPC reported receiving objections from several of its European counterparts. Norway's data protection authority Datatilsynet lodged at least one such [objection](#), calling for fines in addition to the ban on future activity. The Norwegian authority justified additional sanctions given Meta's "particularly serious" violation of EU rules by continuing to transfer data under SCCs after the landmark *Schrems II* ruling in which the European Court of Justice invalidated the EU-U.S. Privacy Shield. The Irish DPC now must resolve objections to its decision or potentially trigger a formal EU dispute resolution mechanism, which could add further delay to a final decision.

- **CJEU Rules on Special Categories of Personal Data.** On August 2, Europe's top court [ruled](#) that the publication of the name of a spouse or partner amounted to the processing of sensitive data because it could reveal sexual orientation. The court explained that such data disclosure falls under the special categories of personal data in Article 9 of the GDPR after consulting Article 4(15) provisions for "data concerning health."

Troutman Pepper Team Spotlight: Jonathan Ishee

Jonathan advises clients at the intersection of technology and health care. His well-rounded perspective is informed by an in-depth understanding of the law, as well as his in-house, government, and academic experiences. As a certified information privacy professional (CIPP), Jonathan offers particular depth in the issues involving the application of technology to the delivery of health care. Jonathan regularly guides clients through the

complexities involved with telehealth; data privacy and security; HIPAA; reimbursement; managed care contracting; CMS; state insurance licensing, fraud, and abuse; and the corporate practice of medicine. He assists clients with the creation of HIPAA and HITECH compliance strategies and their incident response plans. Clients across a range of industry sectors also seek Jonathan's advice on international privacy law, including GDPR, and regulations related to research and employee data.

In addition to his legal practice, Jonathan also serves as an assistant professor of biomedical informatics at the University of Texas Health Science Center at Houston.

Upcoming Events

- Ron Raether (Speaker), "[Testing Screening Operations for Potential Unintended Discrimination](#)," PBSA, September 12, 2022.
- Kim Phan (Speaker), "[Data Ownerships and Security](#)," LEND360, September 12, 2022.
- Kim Phan (Speaker), "[The Shifting Data Privacy and Data Protection Landscape](#)," MBA's Regulatory Compliance Conference, September 19, 2022.
- Ron Raether (Speaker), "[How 2020 Vision Has Blurred Attorney Client Privilege in Incident Response](#)," Infosec World, September 27, 2022.
- Kim Phan (Speaker), "[State Privacy Law Developments](#)," RESPRO'22 Fall Seminar, September 27, 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.
- Joel Lutz (Speaker), "[What's Next in Legislation – How Can We Create Win-Win Scenarios For Consumers & Industry?](#)" LeadsCon, October 25-26, 2022.

Recent Troutman Pepper Regulations

- [The Do's and Don'ts of Cybersecurity Forensic Investigations](#)
- [California ADCA Bill Aims to Increase Children's Data Privacy](#)
- [Proposed New Data Security Rules Could Prove Duplicative, Forcing Banks to Turn over Dangerous Amounts of Secured Data](#)
- [CFPB Turns Its Attention to Data Security – Seven Industry Practices You Need to Know Now](#)

- [According to Banking Industry Groups, CFPB Should Supervise Data Aggregators](#)
- [New York Department of Financial Services Proposes Amendments to Its Cybersecurity Regulation](#)

RELATED INDUSTRIES + PRACTICES

- [Privacy + Cyber](#)
- [eDiscovery + Data Management](#)