Articles + Publications | January 2023

More Privacy, Please – January 2023

WRITTEN BY

Molly S. DiRago | Joshua D. Davey | Natasha E. Halloran | Matthew R. Cali | April Garbuz | Jessica Ring | Kim Phan | Ronald I. Raether Jr. | Robyn W. Lin | Alexandria Pritchett | Andrew Raunau

Editor's Note: *In regulatory news, the Colorado AG published a second version of its proposed regulations. In U.S. litigation, Meta and TikTok both faced further litigation, and an Illinois court ruled that J&M Plating must provide data policies at the time of collection. Additionally, VPPA litigation continued with new suits against The Atlantic and MGM's Online Gaming website. In international news, the EU signed off on an adequacy decision for the EU-U.S. transfer of data, and the OECD signed a new privacy agreement. In very local news, our very own Julie Hoffmeister was promoted to partner!*

US Laws and Regulation

- **Colorado Publishes Second Draft of Privacy Regulations.** On December 21, 2022, the Colorado attorney general (AG) released a second version of the proposed draft rules. Notably, the revised rules no longer require a business to specify its purpose for processing in its privacy notice. Additionally, the rules defined "employment records," which are exempt from the underlying statute. A rulemaking meeting regarding the draft rules will be held on February 1.

- **Indiana AG Sues TikTok.** Indiana AG Todd Rokita filed a pair of lawsuits against TikTok and its Chinese parent company ByteDance Ltd., claiming that TikTok — which it asserts is the most-used app in the U.S. among 13-17 year-olds — made false claims to users of its app. In the first lawsuit, Indiana contends that TikTok lures children onto its platform with representations that it was safe and appropriate for minors, when in reality, the app was a "Chinese Trojan horse" which exposes its users "to non-stop offerings of inappropriate content that TikTok's algorithm force-feeds to them," including sexual content, drug and alcohol references, profanity, and other material not suitable for minors. The second lawsuit alleges that TikTok deceives its users about its information practices, misleading users to believe that the extensive personal information collected by TikTok is protected from the Chinese government and Chinese Communist Party, when in reality TikTok's privacy policy allows it to share that information with its Chinese parent company and other entities subject to Chinese law. The lawsuits seek injunctive relief and civil penalties of up to $5,000 for each violation of Indiana's Deceptive Consumer Sales Act and up to $500 "for each incurable deceptive act committed by" TikTok.

- **Judicial Privacy Bill Passes.** On December 16, 2022, the Daniel Anderl Judicial Security and Privacy Act passed, allowing federal judges to request that data brokers and other internet platforms take down certain categories of personal information and prohibits selling, trading, transferring, or purchasing of judges' personally identifiable information online. The bill honors Judge Esther Salas whose son was shot and killed by a disgruntled litigant after he found her home address online.

- **Senators Look Into FBI's Facial Recognition Practices.** On December 19, 2022, U.S. Senator Jon Ossoff (D-GA), Representative Ted Lieu (D-CA), and Representative Yvette Clarke (D-NY) sent a letter to the FBI, inquiring about its facial recognition practices. The letter focused on First Amendment concerns and requested a full list of FBI-investigated federal offenses using facial recognition and the number of times facial recognition was used for each type of offense. The letter also asked for a full list of offenses when state and local police

used the FBI's Next Generation Identification-Interstate Photo system in their investigations. The letter further raised Fourth Amendment concerns and requested FBI policies on the use of facial recognition and oversight over its use by state and local police.

US Litigation and Enforcement

- **Trade Association Sues California Over Age-Appropriate Design Code.** On December 14, 2022, NetChoice filed a complaint against the California AG, alleging that the California Age-Appropriate Design Code Act (CAADCA or AB 2273) is facially unconstitutional. The complaint alleged that "the law imposes on private firms, big and small, the obligation to identify and 'mitigate' speech that is 'harmful or potentially harmful' to users under 18 years old," which would "press[] companies to serve as roving censors of speech on the Internet." Signed into law in September 2022 and scheduled to take effect in July of 2024, the CAADCA will help protect the wellbeing, data, and privacy of children using online platforms by requiring businesses subject to the CAADCA to implement added safety features and data privacy measures on their platforms for California children. NetChoice's complaint asked (1) the court to preempt the CAADCA via the COPPA and the commerce clause; (2) declare the CAADCA unconstitutional under the California Constitution; and (3) enjoin the AG from "taking any action to enforce" the CAADCA.

- **Meta Judge Proposes *Cy Pres* Distribution Instead of Payments to Class Members.** On December 15, 2022, Northern District of California Judge James Donato declined to grant preliminary approval of Meta's $37.5 million settlement to a putative class of approximately 70 million members, noting any benefit to class members was outweighed by the settlement administration costs, and the proposed attorney's fees were inflated. The litigation stemmed from claims that Meta violated its own privacy policy by collecting, storing, and monetizing users' location data for targeted advertisements on Facebook, even after the users turned off location services on their mobile devices. Judge Donato recommended the parties consider a *cy pres* distribution, directing the parties to identify potential *cy pres* recipients, and proposed that the parties select organizations that enhance access to the internet and technology for disadvantaged populations.

- **Alleged Deficient Security Measures Exposes Customers' Information.** On December 2, 2022, Debt Cleanse Group Legal Services LLC filed a class-action complaint against GoTo Technologies USA, Inc. and LastPass US LP to recover damages, restitution, and injunctive relief after an August 2022 data breach of its customers' information. The complaint alleged that the defendants' "unreasonable data security practices, monitoring, and unreasonable aggregation and integration of Plaintiff's and Class members' Customer Information" resulted in hackers gaining unauthorized access and possession of customer information. Debt Cleanse further claimed that the defendants unreasonably delayed their provision of notice of the incident. Debt Cleanse contended that there is a strong probability that entire batches of stolen customer information have or will be placed on the black market, which may increase the risk of fraud and identity theft.

- **Facebook Users Allege Meta Collected Their Tax Information.** On December 1, 2022, two anonymous Facebook users filed a class-action complaint against Meta Platforms, Inc. for collecting, without their consent, sensitive information from tax filing websites H&R Block, TaxAct, and Tax Slayer. The plaintiffs claimed that the company recorded their information from tax returns via a "pixel" — a piece of code that logs users' activities on third-party websites and sends the details back to Meta. The information allegedly collected included their names, email addresses, adjusted gross incomes, tax-filing statuses, refund amounts, dependents' names, and college scholarship amounts. The plaintiffs also alleged that Meta made no effort to enforce the promise in its user contract that the company requires third parties using the pixel to have lawful rights to collect, use, and share the data before providing any data to Meta.

- **Atlantic Subscribers Claim Magazine Shares Data With Meta.** On December 12, 2022, subscribers filed a class-action complaint against *The Atlantic* for allegedly disclosing subscriber data to Meta in violation of the Video Privacy Protection Act (VPPA). The VPPA prohibits videotape service providers from disclosing personally identifying customer information to a third party without their informed, written consent. As purported in the suit, private personally identifiable information was transmitted to Facebook's parent company through

Meta Pixel, a user tracking tool embedded in *The Atlantic's* website. When a viewer watches a video on a website with Meta Pixel installed, the viewer's Facebook ID and the name of the video are transmitted to Meta. According to the complaint filed in California federal court, the plaintiffs and other *Atlantic* users never received a consent form, specifying these data disclosure practices, nor did *The Atlantic* request user consent.

- **NBA Moves to Dismiss VPPA Class Action.** Plaintiff Michael Salazar filed a proposed class action against the National Basketball Association (NBA), arguing that the company violated the VPPA by sharing NBA website information with Meta. On December 2, 2022, the NBA filed a motion to dismiss, arguing that the complaint seeks to "impose potentially enormous liability … for utterly routine internet browsing activities." The motion argued that Salazar is not a renter, purchaser, or subscriber of NBA video tape services; the NBA did not knowingly disclose personally identifiable information about him, and the plaintiff consented to any alleged disclosures. The NBA also contended that Salazar's allegations fall outside any plausible interpretation of the VPPA. On December 22, 2022, the court stayed discovery due to the likely breadth of discovery in the case, no prejudice from the delay, and the defendant's motion to dismiss raised "substantial issues" that could result in dismissal, including whether the court had subject matter jurisdiction and whether the plaintiff consented to the conduct.

- **Illinois Court Rules BIPA Requires Data Policies Up Front.** An Illinois appellate court held that under the state's Biometric Information Privacy Act (BIPA), a company must establish publicly available rules for storing and destroying biometric data no later than the same day the company comes into possession of the data. Under Section 15(a), a private entity "in possession of biometric […] information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying […] biometric information." In a putative class-action lawsuit brought by former employees against J&M Plating, J&M argued that because Section 15(a) contains no timing language for the creation and distribution of the schedule and because no harm occurred to the plaintiffs, it did not violate BIPA. J&M did not create a schedule until nearly four years after it began collecting employee data. The Second District three-judge panel disagreed, finding "no rational reason" the Illinois legislature would intend to develop a schedule after Section 15(b)(2)'s notice requirement, which occurs prior to collection.

- **MGM's Online Gambling Site Sues Over Customer Data Leak.** On December 22, 2022, a putative class-action lawsuit was filed against BetMGM for a data breach, compromising the personal identifying information of its customers. BetMGM, a sports betting website owned by casino and hotel group MGM Resorts International, discovered the breach on November 28, 2022, and notified customers of the situation on December 21, 2022. In the email sent to affected customers, BetMGM stated that the breach occurred in May 2022, and their "name, contact information, date of birth, hashed Social Security number, account identifiers and information related to your transactions" were obtained in an "unauthorized manner." The suit alleged that BetMGM "intentionally, willfully, recklessly or negligently" failed to encrypt customer data or store it in a secure location. The plaintiffs also sued for both breach of implied contract and negligence, asking the New Jersey court for a declaratory judgment.

- **Tax Prep Co. Files Lawsuit Over Data Breach Affecting 240K Clients.** After a data breach affected over 240,000 of its customers, tax service provider Wing Financial was sued in Oklahoma federal court. The class-action complaint alleged that a cybersecurity attack exposed consumers' highly sensitive personally identifiable information, and the tax service provider did not alert customers to the breach until four months after discovering the attack. The plaintiff, an Oklahoma resident and Wing Financial customer, claimed that the data breach directly resulted from Wing Financial's "failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PII," seeking judgment against the company for negligence, negligence per se, breach of fiduciary duty, unjust enrichment, breach of implied contract, and a violation of the Oklahoma Consumer Protection Act. The plaintiff also requested equitable relief, compelling Wing Financial to use suitable methods and policies related to consumer data collection, storage, and safety, as well as to specify the type of PII compromised during the attack. The plaintiff further sought an order, requiring the tax service provider to pay for at least seven years of credit monitoring services for all class members.

- **Respondus Possibly Faces Cross-Claim in BIPA Lawsuit for Its Online Proctoring Software.** On December 12, 2022, Lewis University filed a motion, seeking leave to file a cross-claim against co-defendant Respondus, Inc. in a class-action lawsuit related to its online proctoring software Respondus Monitor. The underlying lawsuit — filed in Illinois federal court in November 2020 by Lewis University students allegedly required to use Respondus Monitor — claimed Lewis University violated BIPA by failing to disclose or obtain written consent before collecting, capturing, or storing students' biometric data. Lewis University now would like to file contribution, implied indemnity, and equitable estoppel cross-claims against Respondus, arguing that Respondus should take responsibility for any damages. Respondus opposed the motion, and on December 23, 2022, moved to stay all case deadlines, pending settlement in a related BIPA action filed against Respondus in Illinois federal court.

- **New Putative Class Actions Allege TikTok Violates Wiretapping Act.** Five new class actions — filed in Illinois, California, New Jersey, New York, and Pennsylvania — all alleged TikTok surreptitiously intercepted the electronic communications of its users in violation of the Federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq.* The suits claimed TikTok used JavaScript computer code to track users' "every move" (including keystrokes, clicks, scrolling, finger movements, and text). Specifically, the plaintiffs alleged that TikTok collected this data when a user opened a third-party website because the website opened in a TikTok's in-app web browser as opposed to opening in the phone's standard web browser.

International Regulation and Enforcement

- **European Commission Announces Adequacy Decision for EU-US Data Flows.** On December 13, 2022, the European Commission began adopting an adequacy decision for the EU-U.S. Data Privacy Framework after the *Schrems II* decision in July 2020. Significantly, the adoption demonstrates that the European Commission believes the framework provides comparable safeguards to those in the EU. Under the draft decision, US companies can join the EU-U.S. Data Privacy Framework by committing to comply with a detailed set of privacy obligations, and EU citizens can access several redress avenues if their personal data rights are violated. The decision also provides for a number of limitations and safeguards regarding the access to data by U.S. criminal law enforcement and for national security purposes.

- **OECD Signs Privacy Agreement.** On December 16, 2022, the Organization for Economic Cooperation and Development (OECD) published a new transnational agreement to help safeguard user privacy in situations related to national security and law enforcement purposes. Signed by 38 OECD countries, including the U.S. and the U.K., the agreement will help enable data flow between countries. The agreement arose out of a 1980 recommendation (completed in 2021), which identified policy gaps affecting the cross-border flow of personal data. The gaps included a lack of "common articulation at the international level of the safeguards that countries put in place to protect privacy and other human rights and freedoms when they access personal data held by private entities in the course of fulfilling their sovereign responsibilities related to national security and law enforcement."

Troutman Pepper Team Spotlight: Julie Hoffmeister

Newly promoted Richmond Partner Julie Hoffmeister focuses her practice on financial services litigation. As part of the firm's national practice, Julie defends all types of consumer-facing companies in individual claims and class actions, including claims under the Fair Credit Reporting Act (FCRA), the Fair Debt Collection Practices Act (FDCPA), the Telephone Consumer Protection Act (TCPA), the Uniform Commercial Code (UCC), and the Driver's Privacy Protection Act (DPPA). Julie leverages her litigation knowledge to assist businesses in

developing compliance processes and procedures.

Recently engaged in December 2022, Julie currently spends all her free time wedding and honeymoon planning and playing with her golden retriever puppy Kiki.

Recent Webinars, Podcasts, and Events

- Kim Phan (Speaker), “Dark Patterns and Commercial Surveillance — What You Need to Know,” ACA Huddle, December 21, 2022.
- Kamran Salour and Sadia Mirza (Speakers), “Board-er Patrol in Privacy and Cyberattacks,” *Unauthorized Access* Podcast, January 4, 2023.
- Ron Raether (Speaker), “CFPBs Involvement in Tenant Screening,” *FCRA Focus* Podcast, January 5, 2023.

Recent Troutman Pepper Publications

- TikTok Faces ‘Pile-On’ Pressure From States After Indiana Sues

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management