Articles + Publications | January 2022

# More Privacy, Please – January 2022

**WRITTEN BY**

Molly S. DiRago | Sadia Mirza | Christopher J. Capurso | Mary Kate Kamka | Jack Altura | Graham T. Dean | Lissette Payne | John Sample | Robyn W. Lin

***EDITOR'S NOTE*:** There was no respite in privacy and cyber law in December 2021, despite the holidays and COVID-19 case surge. **Domestically**, U.S. regulators stepped up their efforts, signaling their focus on privacy policies (FTC) and security incident notification (federal banking agencies); meanwhile Democratic senators urged the CFPB to take a more proactive stance with consumer reporting agencies. In U.S. litigation, Illinois' biometric statute (BIPA) continued to take center stage, as did FTC settlements with companies accused of deceptive practices related to privacy. **Internationally**, facial recognition company Clearview AI took the heat from several countries over its database of billions of images scraped from the internet. Grindr found itself in a similar position, as the Norwegian Data Protection Authority issued a $17m+ fine against it, and a similar complaint was filed in Austria. Apple, too, may soon find itself on the chopping block, as Poland's Office of Competition and Consumer Protection investigated the privacy protections embedded in its new iOS. Finally, the UAE issued its first federal data protection law, effective January 2.

## US Laws and Regulation

- **FTC Rulemaking Announcement.** On December 10, 2021, the Federal Trade Commission (FTC) filed an Advanced Notice of Proposed Rulemaking with the Office of Management and Budget on amendments under FTC Act Section 18, which allows the FTC to prescribe particular acts and practices as deceptive or unfair. Advanced notices help agencies solicit stakeholder comments before carrying out an official rulemaking process. The FTC indicated this proposed rulemaking would address privacy practices, including bias in algorithmic rulemaking, and curb lax security practices. Despite not publishing any additional information on the rulemaking beyond this summary, the FTC did establish a date of February 2022, indicating it will either start soliciting comments or official rulemaking will begin next month.

- **Think Fast: Banking Regulators Release Final Computer-Security Incident Notification Requirements.** On November 18, 2021, federal banking agencies issued a final rule, establishing data security incident response notification requirements for "banking organizations" and "bank service providers." The rule included a headline-grabbing, 36-hour regulatory notification requirement for banking organizations. Despite the stringent timing requirement, a relatively high threshold for what constitutes a reportable "notification incident" eases the final rule's practical burden. This rule also requires that bank service providers notify banking organizations "as soon as possible" after experiencing an incident considered "reasonably likely to materially disrupt or degrade covered services … for four hours or more." These requirements will take effect on April 1, and entities should begin analyzing their breach response procedures now to ensure timely compliance. To read more about this and the final rule, click here.

- **Democratic Senators Urge CFPB to Act on Credit Reporting Errors.** On November 10, 2021, a group of Democratic senators sent a letter to Consumer Finance Protection Bureau (CFPB) Director Rohit Chopra, requesting that the CFPB take a proactive stance in its regulation of consumer reporting agencies (CRAs). The group, led by Sen. Brian Schatz (D-HI) and includes Sens. Elizabeth Warren (D-MA) and Sherrod Brown (D-OH), urged the CFPB to take immediate action to evaluate errors and ensure equity in credit reporting, while also making specific suggestions on how to do so. Some of those suggestions are summarized further here.

- **US Defense Department Hires First Artificial Intelligence Chief.** On December 8, 2021, the deputy secretary of defense established the position of chief digital and artificial intelligence officer in the Department of Defense (DOD) effective February 1. The senior official will report directly to the deputy defense secretary and will oversee the strengthening and integration of data, artificial intelligence, and digital solutions in the DOD. This move reflects the DOD's increased emphasis on the advancement of data and technology integration.

## US Litigation and Enforcement

- **Seventh Circuit Asks Illinois Supreme Court for Guidance on BIPA Accrual Issue.** On December 20, 2021, the Seventh Circuit Court of Appeals issued a long-awaited decision in *Cothron v. White Castle*, punting on the pivotal question of when a claim accrues under Illinois' Biometric Information Privacy Act (BIPA). Acknowledging that it is "genuinely uncertain" about how to rule on this state-law issue, the Seventh Circuit certified the question to the Illinois Supreme Court. When resolved, this issue will dictate the timeliness of the *Cothron* suit and many others in which the initial alleged BIPA violation precedes the applicable limitations period (the Illinois Appellate Court recently addressed the applicable statute of limitations period in *Tims v. Black Horse Carriers*). Essentially, Cothron posits that each time her biometric information was collected, White Castle violated BIPA; White Castles argues that only the initial collection constituted a violation. This also will impact the amount of exposure for defendants, as BIPA provides for statutory damages between $1,000 and $5,000 for every violation.

- **Amazon and Microsoft File Motions to Dismiss Lawsuits Alleging Illinois BIPA Violations.** Amazon and Microsoft both filed separate motions for summary judgment regarding their respective lawsuits, alleging violations of the Illinois BIPA, which requires companies to receive consumer consent before collecting or processing biometric information of Illinois residents. The lawsuits allege that both companies obtained a faceprint database (Diversity in Faces) from IBM, and both companies used this database to improve their facial recognition applications. In response to the allegations, the companies argue that the BIPA did not apply because all alleged biometric data analysis occurred outside the state of Illinois.

- **FTC Finalizes Order Banning Stalkerware Provider From Spyware Business.** In its September 2021 complaint, the FTC alleged that Support King LLC (formerly SpyGone.com) sold stalkerware apps that allowed purchasers to surreptitiously monitor photos, text messages, web histories, GPS locations, and other personal information on the phone with the installed app without the device owner's knowledge. In December 2021, the

FTC finalized the settlement, agreed to by FTC commissions in a 4-0 vote, which prohibits further sale or advertising of stalkerware by SupportKing and mandates deletion of all personal data collected using the company's app.

- **OpenX Reaches $2M Settlement With FTC on COPPA Violation Allegations.** The FTC and OpenX reached a settlement on alleged violations of the Children's Online Privacy Protection Act (COPPA) and FTC Act. The FTC alleged that OpenX, a California-based online advertising platform, violated COPPA by collecting data on children under the age of 13 without parental consent. The FTC also alleged that OpenX violated the FTC Act by offering an opt-out for geo-location data but not honoring that opt-out choice. The settlement requires OpenX to pay a $2 million fine, delete all ad request data collected to serve targeted ads, and implement a COPPA compliance program.

- **MyLife.Com and CEO Settle With FTC for $21M.** On December 15, 2021, a California District Court approved and entered a stipulated order of judgment, resolving claims between the FTC and MyLife.com, Inc. and its CEO, Justin Tinsley. The Department of Justice, on behalf of the FTC, originally filed a complaint against MyLife and Tinsley, alleging that MyLife deceived consumers by misleading them about the content of its background reports and its billing practices. The complaint further alleged that MyLife was a credit reporting agency (CRA) and that its conduct violated the Fair Credit Reporting Act (FCRA). The settlement requires MyLife to pay $21 million and institute an FCRA compliance program.

- **Company's Director Sued in His Individual Capacity for TCPA Violations.** In *Zoppi v. Proform Trading LLC*, the District Court of New Jersey granted the plaintiff's motion to amend his complaint to bring Telephone Consumer Protection Act (TCPA) claims against Proform Trading and its director in his individual capacity. Following decisions from the Third Circuit and Northern District of Texas, the court agreed that a corporation's officer may be held personally liable under the TCPA if he had "direct, personal participation in or personally authorized the allegedly unlawful conduct." For more information, click here.

## International Regulation and Enforcement

- **Pressure Mounts on Facial Recognition Company Clearview AI.** Countries are increasingly setting their sights on Clearview AI, a facial recognition company accused of creating and maintaining a database of more than three billion images scraped from the internet from which it matches photographs of people against the images. This allegedly occurs without the consent of the subjects of the photographs.

### Canada

- **Canadian Provinces Order Clearview AI to Stop Collecting, Using, and Disclosing Images Scraped From Internet.** On December 14, 2021, privacy authorities from the Canadian provinces of British Columbia, Alberta, and Quebec ordered Clearview AI to stop offering its facial recognition services; stop collecting, using, and

disclosing images of people; and to delete images and biometric facial arrays. The orders are limited to these three provinces. Privacy Commissioner Daniel Therrien of the Office of the Privacy Commissioner of Canada, a participating entity in the Clearview investigation, welcomed the actions taken by its provincial counterparts, and stated that "[t]hese orders also highlight once again significant shortcomings with the federal private sector privacy law."

**France**

- **France Threatens Fine Against Clearview AI.** On December 16, 2021, the French data protection watchdog (CNIL) formally ordered Clearview AI to delete its facial recognition database of images within two months and to stop collecting data. The agency stated the company violated the European Union's General Data Protection Regulation (GDPR) by collecting and using biometric data without a legal basis. The watchdog also cited Clearview AI's failure to adequately and effectively address the rights of individuals, including data subject access requests (DSARs). Clearview AI maintains it is not bound by the GDPR.

**United Kingdom**

- **ICO Issues Provisional Fine Against Clearview AI for Over £** The U.K.'s Information Commissioner's Office (ICO) announced a provisional intent to impose a fine of just over £ 17 million (roughly $19.1 million USD) against Clearview AI. The announcement comes after a joint investigation between the ICO and the Office of the Australian Information Commissioner (OAIC), which found Clearview likely failed to comply with U.K. data protection laws, including (1) failing to process information in a way people are likely to expect or that is fair; (2) failing to have a process in place to stop data from being retained indefinitely; (3) failing to have a lawful basis for collecting the information; (4) failing to meet the higher protection standards required for biometric data (classed as 'special category data' under the GDPR and the U.K. GDPR); and (5) failing to provide information concerning the processing of the data.

- **Norway's Privacy Watchdog Fines Grindr $7 Million.** The Norwegian data protection agency recently fined dating app Grindr $7.17 million for illegally sharing user data with advertisers. The fine comes after the Norwegian Consumer Council, along with the European-based nonprofit organization None of Your Business (NOYB), filed a complaint in January 2020, alleging the app unlawfully shared personal data with third parties for marketing purposes. Initially set at $11.7 million, the fine was reduced after the agency determined the company improved its methods for obtaining consumer consent. NOYB also filed a separate complaint in Austria last month.

- **Poland's Office of Competition and Consumer Protection to Investigate Apple's Privacy Policy.** The Office of Competition and Consumer Protection (UOKIK) announced that it will investigate whether Apple is violating Poland's new rules on privacy and personal data processing for iOS devices. In April 2021, Apple updated its iOS operating system with new privacy controls designed to limit digital advertisers from tracking iPhone users. UOKIK suggests that Apple's new iOS significantly reduces the ability of third-party apps to

obtain personal data to send personalized advertisements to iPhone users. According to UOKIK President Tomasz Chrostny, the regulatory agency wants “to examine whether Apple’s actions may be aimed at eliminating competitors in the market for personalized advertising services, the objective being to better sell their own service.”

- **CNIL Publishes White Paper on Digital Payments and Data Privacy.** The French Data Protection Authority (CNIL) published a white paper, discussing how companies can comply with data privacy and security obligations. The white paper focuses on various key topics, including GDPR compliance as a customer trust factor, the preservation of anonymity of mobile payments, and confidentiality of transactions in the digital euro project. The white paper also sets out its expectations and guidance on several key data protection issues, including proportionality and data minimization; identification and biometric data; ensuring actors are properly characterized as data controllers, data processors, or joint controllers; confirming the appropriate legal basis exists for each processing activity; and the security of payment data.

- **UAE Issues First Federal Data Protection Law.** The United Arab Emirates Cabinet Office recently announced Federal Decree-Law 45 of 2021 (the Data Protection Law), one of the first projects of UAE’s legislative reform, which became effective on January 2. The Data Protection Law creates a framework to ensure confidentiality and to protect the privacy of individuals by requiring organizations to implement policies and procedures for the management and protection of personal data.

## Troutman Pepper Team Spotlight: Sadia Mirza

As a member of Troutman Pepper's Cybersecurity, Information Governance, and Privacy team, Sadia Mirza dedicates her practice to counseling clients on cutting-edge privacy and cybersecurity issues. Clients turn to her for compliance counseling, pre-incident response planning and preparedness, and also call her when the first sign of a security incident/data breach appears. Given her years of experience coaching clients through security incidents, Sadia is heavily involved with data breach regulatory and litigation matters, giving her a 360-view and understanding of the issues most important and relevant to her clients.

Sadia brings extensive experience in data security and privacy matters, having handled a number of data breaches and investigations in a variety of industries. Clients trust her to guide them through all aspects of incident response, including handling immediate forensics investigations, coordinating initial crisis management, and complying with state and federal notification requirements. She also has experience defending companies under investigation by the Federal Trade Commission, attorneys general offices, and other regulatory authorities.

Sadia is a Certified Information Privacy Professional in the United States (CIPP/US) and a Certified Information Privacy Manager (CIPM) for the International Association of Privacy Professionals (IAPP). Recently, IAPP appointed Sadia to its Women Leading Privacy Advisory Board effective January 1. Her experience, leadership, and frequent media contributions on new and emerging privacy and data security laws makes her a well-recognized thought leader in the field, which she showcases by serving on numerous privacy and cybersecurity panels throughout the U.S.

Lastly, but most importantly, Sadia enjoys spending her time with her three girls — Maryam, Ammarah, and Fatima. "Mama" will always be her favorite title.

---

## Webinars

- **Attorney Client Privilege in Incident Response | Tuesday, February 1, 2022 | 1:30 p.m. ET**

  Troutman Pepper Partner Ron Raether will moderate a panel on "Attorney Client Privilege in Incident Response" during NetDiligence's *Cyber Risk Summit* in Fort Lauderdale, FL. For more information and to register, please click here.

## RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management