Articles + Publications | May 2022

More Privacy, Please – May 2022

WRITTEN BY

Molly S. DiRago | Ronald Raether, Jr. | James Koenig | David N. Anthony | Angelo A. Stio, III | Ashley L. Taylor, Jr. | Robyn W. Lin | Lissette Payne | Jonathan "Grady" Howe | John Sample | Gerar Mazarakis | Kamran Salour

Editor's Note: Connecticut became the fifth state in the nation to successfully pass a comprehensive privacy bill (now awaiting its governor's signature), following California, Colorado, Utah, and Virginia. Meanwhile, Kentucky passed a Genetic Privacy Bill, aimed at "direct-to-consumers" genetic testing companies, and Louisiana introduced its own comprehensive privacy bill. At the federal level, Congressman Ted W. Lieu introduced a bill, amending Section 2703 of the Stored Communications Act, which would require government entities to obtain a warrant to access a customer's metadata. The Department of Commerce appointed 27 members to the National Artificial Intelligence Advisory Committee, and the Better Business Bureau launched a TeenAge Program Privacy Program to help companies collect and manage teenage data responsibly. On the litigation side, the Department of Justice announced its first-ever False Claims Act (FCA) settlement under the context of its newly instituted Civil Cyber Fraud Initiative. Illinois continues to generate litigation, including a class action against luxury brand Louis Vuitton; a class action against a well-known convenience store; and a new holding, clarifying that the Biometric Information Privacy Act governs biometric information derived from photographs. Internationally, Europe is poised to adopt the Digital Services Act and the Digital Markets Act, and the Dutch Privacy Authority announced its largest fine to date.

US Laws and Regulation

- **Connecticut's Comprehensive Privacy Bill Passes Both Houses.** On April 28, the Connecticut House passed Senate Bill 6, an act concerning personal data privacy and online monitoring. The bill would provide consumer rights, including (1) the right to access one's own data; (2) the right to correction; (3) the right to deletion; (4) a portability right; and (5) the right to opt out of the processing of personal data for the purposes of sale, targeted advertising, or profiling. The bill now awaits the governor's signature. If passed, it would go into effect on July 1, 2023, with certain exceptions. To read more, click here.

- **Kentucky Passes Genetic Privacy Bill.** On April 8, Kentucky Governor Andrew Beshear signed the Genetic Information Privacy Act (House Bill 502) into law. The bill would require "direct-to-consumer genetic testing companies" — companies that offer genetic testing or services to consumers — to obtain consumers' consent for the collection, use, or disclosure of their genetic data. The bill also requires such companies to provide a process for consumers to access their genetic data; delete their account and genetic data; and request and obtain the destruction of their biological samples. Enforced by the Kentucky attorney general, the bill does not contain a private right of action. To read more, click here.

- **Introduction of Warrant for Metadata Act.** On April 20, Congressman Ted W. Lieu (D-Los Angeles County)

introduced legislation that would require governmental entities to obtain a warrant before requesting that an electronic communications provider disclose a customer's metadata. This act would amend Section 2703 of the Stored Communications Act (SCA), which protects some electronic communications from unauthorized disclosure, to include metadata also stored electronically. To read the press release, click here.

- **Louisiana Introduces Comprehensive Privacy Bill.** On April 5, Louisiana Representative Daryl Deshotel introduced House Bill 987, the Louisiana Consumer Privacy Act. The bill would provide consumers with rights, including (1) the right to confirm whether a controller is processing the consumer's personal data; (2) the right to access their data; (3) the right to obtain a copy of the consumer's personal data; (4) the right to delete the data; and (5) the right to opt out of the processing of the consumer's personal data for targeted advertising or the sale of personal data.

- **New Jersey Employers Must Notify Employees When Using Tracking Devices.** On April 18, a New Jersey law that governs employers' use of tracking devices on vehicles used by employees went into effect. Under this act, any employer who "knowingly makes use of a tracking device on a vehicle used by an employee" must first provide written notice to the employee. The act does not apply to certain employees, such as the Department of Corrections, State Parole Boards, or any public transportation companies. The act also does not distinguish between employer-owned vehicles and employees' personal vehicles.

- **Commerce Department Appoints 27 Members to National AI Advisory Committee.** On April 14, the U.S. Department of Commerce announced the appointment of 27 experts to the National Artificial Intelligence Advisory Committee (NAIAC). These appointments are the first for the recently established committee, which was created in response to the National AI Initiative Act of 2020. The committee will advise the president and the National AI Initiative office on a variety of AI-related issues, including the current state of U.S. AI competitiveness, the state of science around AI, and AI workforce issues. Nominated by the public, committee members come from a broad range of AI-relevant disciplines in industry, academia, civil society, and nonprofits. Committee members will serve three-year terms and may serve two consecutive terms at the discretion of the secretary.

- **BBB National Programs Rolls Out Teen Privacy Program Roadmap.** In an effort to provide companies with an operational framework for addressing teen privacy, the BBB National Programs' Center for Industry Self-Regulation (CISR) published its TeenAge Privacy Program Roadmap (TAPP). The CISR acknowledged the importance of the roadmap at a time where there is a heightened focus on children's and teen privacy with little to no guidance specific to the teen audience. The CISR also noted that while data privacy and safety practices that protect adult consumers provide a firm foundation for teens, they simultaneously run the risk of being insufficient to respond to the unique needs of teens since privacy issues that affect adults may be more impactful, and sometimes altogether unique, to teenagers. The CISR conducted a study, finding that teen-directed apps are more likely to engage in ad serving; include more third-party trackers; ask for more permissions; and offer more in-app purchases than apps developed for a general user audience, which greatly increases the attack surface for privacy risks.

- **Colorado Releases Pre-Rulemaking Guidance for CPA.** The Colorado Office of the Attorney General (COAG) released pre-rulemaking guidance for the Colorado Privacy Act (CPA). The COAG released five principles to help implement the CPA: (1) promoting consumer rights; (2) clarify ambiguities; (3) facilitate

efficient and expeditious compliance; (4) harmonize the CPA with competing protections and obligations from other privacy frameworks; and (5) allow for innovation. Additionally, the COAG also released targeted topics on which the COAG believes informal feedback would be helpful: (1) the universal opt-out; (2) consent; (3) dark patterns; (4) data protection assessments (DPAs); (5) profiling; (6) opinion letters and interpretive guidance; (7) offline and off-web collection of data; (8) protecting Coloradans in a national and global economy; and (9) any other additional CPA-related topics. The CPA comment portal is available here.

US Litigation and Enforcement

- **Federal Contractors on Notice After DOJ Announces First Civil Cyber Fraud Initiative Settlement.** DOJ agreed to its first-ever False Claims Act (FCA) settlement under its newly instituted Civil Cyber Fraud Initiative. Among other things, the initiative employs the False Claims Act as an avenue to pursue cybersecurity-related fraud by government contractors and grant recipients. The $930,000 settlement with Comprehensive Health Services (CHS) is a watershed moment in the department's approach to cybersecurity, highlighting its renewed focus and commitment to holding vendors doing business with the federal government accountable for meeting federal cybersecurity requirements. For further analysis and discussion, click here.

- **Chicago Holiday Inn Strikes $503K Deal to End BIPA Suit.** On April 18, an owner of a Chicago Holiday Inn entered into a settlement that would pay more than $503,000 to resolve allegations under Illinois' Biometric Information Privacy Act (BIPA). The suit alleged that the company required employees to follow biometric timekeeping practices that violated their privacy rights by requiring them to scan their fingerprints when clocking in and out of shifts to track their work hours. Led by lead plaintiff Thomas Robertson, the class includes 402 employees.

- **BIPA Covers Photograph-Derived Facial Information.** On April 25, an Illinois judge held that BIPA governs photograph-derived facial information and denied a motion to dismiss by defendant software maker Onfido, Inc. The class action alleges that Onfido violates BIPA by scanning uploaded photographs and extracting biometric identifiers without consent. Onfido argued that because it was scanning a *photograph* and not a person's face, BIPA did not apply. The court disagreed, concluding that "the information Onfido allegedly obtains plausibly constitutes a scan of face geometry," which qualifies as a biometric identifier under BIPA.

- **Louis Vuitton Faces Class-Action BIPA Lawsuit Over Virtual "Try-On" Tool.** On April 8, plaintiff Paula Theriot filed a class-action lawsuit against Louis Vuitton for violating Illinois' BIPA with its virtual "try-on" application on its website. The complaint alleges that Louis Vuitton encourages its consumers to virtually try on their sunglasses by providing Louis Vuitton with complete facial scans and images of their face — sensitive biometric identifiers — without obtaining appropriate consent or being informed of the biometric data collection. The plaintiff alleges she never signed a written release, authorizing the biometric data collection or that she was informed about the purpose for collecting her biometric data. Furthermore, the website's terms and conditions did not indicate that any biometric information would be collected. The complaint also alleges that Louis Vuitton did not publish a public policy, stating the data retention procedures for biometric data.

- **National Convenience Store Chain Faces BIPA Class Action By Shoppers Over Facial Scans.** A class of shoppers have alleged that a chain of national convenience stores captures and stores their biometric data,

using facial recognition technology without first obtaining their informed consent or providing data retention schedules in violation of BIPA. The suit alleges that the chain uses a surveillance system in its stores called Click-it, Inc. that are equipped with facial recognition software to, among other things, identify repeat customers. The chain also has a patent for its own facial recognition system, which would provide a contactless checkout process involving shoppers to enter the store, take whichever items they'd like, and leave without checking out with a cashier.

- **Ninth Circuit Re-Affirms Preliminary Injunction Against LinkedIn.** The Ninth Circuit re-affirmed the district court's decision to grant a preliminary injunction against LinkedIn, enjoining the social media company from denying hiQ access to its website. hiQ's business model involves "scraping" publicly available data from public LinkedIn profiles. The Ninth Circuit previously affirmed the preliminary injunction before the Supreme Court vacated and remanded in light of its decision in *Van Buren v. United States*, 141 S. Ct. 1648 (2021). For more analysis, please click here.

- **Data Broker Sued Over Alleged Customer Privacy Violations.** Drivers filed a class action against data broker Otonomo, alleging that it harvests location data to pinpoint where people likely live, work, and worship in violation of the California Invasion of Privacy Act. Lead plaintiff Saman Mollaei claims he purchased a 2020 BMW X3, containing an electric device that allowed Otonomo to track the car's real-time location without Mollaei's consent. Otonomo allegedly collects 4.3 billion data points a day and sells this data to thousands of organizations that paid for such access.

- **Class-Action Lawsuit Members Oppose $92M TikTok Settlement.** TikTok users in America filed a class action against the social media platform, alleging that it secretly collected user data and shared it with the Chinese government. Class members also alleged a potential BIPA violation after the cases were consolidated in Illinois. Objections included arguments that class counsel failed to file the fee petition before the objection deadline and that minor class members received insufficient notice and were not represented separately during settlement negotiations.

International Regulation and Enforcement

- **Europe Poised to Enact the Digital Services Act.** Under the Digital Services Act (DSA), major marketplace and social media platforms must give governments insight into their algorithms and provide users clear avenues to remove abusive content and disinformation. The act also would guarantee access to information about how content is recommended to consumers and would provide consumers better control over the use of their personal data. The act further prohibits targeted advertising aimed directly at minors. Now going through the final stages of adoption, the finalized act would become effective no earlier than January 2024.

- **Dutch Data Protection Authority Announces Largest Fines to Date.** On April 12, the Dutch Data Protection Authority (DDPA) imposed a fine of 3.7 million euros on the Tax and Customs Administration. The fine resulted after years of illegal processing of personal data in the Fraud Signaling Facility (FSV), which maintained a blacklist used to monitor signs of fraud. The administration's own research showed that employees were instructed to base their determinations of who presented a fraud risk on matters, such as people's nationality or appearance. For more information, click here.

- **Germany's BfDI Presents Consultation Report on AI.** On April 4, Germany's Federal Commissioner for Data Protection and Freedom of Information (BfDI) published a report on the use of artificial intelligence in law enforcement and security. According to the report, AI is used despite fundamental legal questions remaining unanswered, and the legislature should timely regulate to create a "comprehensive, empirical and interdisciplinary inventory," ensuring the observation of general data protection principles. Specifically, AI operations should be transparent, enabling human users to understand and trust the system, and the data protection supervisory authorities should be able to comprehensively control AI applications. A comprehensive data protection impact assessment should be conducted before AI is used. The BfDI's report follows a public consultation on the use of AI in law enforcement and security conducted from September 30 to December 17, 2021.

- **Final DMA Text Features Unexpected Changes.** In 2020, the European Commission proposed the Digital Markets Act (DMA) to ensure fair and open digital markets by regulating large online platforms acting as "gatekeepers." On April 14, a final DMA text was circulated, revealing several last-minute changes. Such changes include clarifying legal obligations and making legal challenges more difficult; ensuring users can default to third-party apps and app stores; and addressing potential unfair practices that might develop in the future. Changes also include preventing gatekeepers from using personal data provided to third-party services, operating on the gatekeeper's platform and giving stronger power to the European Commission to determine how interoperability of messaging services should work. The DMA adoption is expected in May 2022, with the compliance process starting in early 2024.

- **Swedish Data Protection Authority Warns of 26% Uptick in Cybersecurity Attacks Impacting Health Care Sector.** The Swedish DPA, the Integritetsskyddsmyndigheten, warned of a significant increase in health care sector cybersecurity attacks in 2021. In total, 5,767 cyber incidents were reported, or approximately 110 incidents a week, to the Swedish DPA. Almost six out of every 10 reported cyber incidents resulted from human error, such as incorrectly sending emails. The Swedish DPA stated that the human error factor behind many of the cyber incidents highlights the need for organizational and technical measures, as well as employee training.

Troutman Pepper Team Spotlight: Jim Koenig

New York-based Partner Jim Koenig co-chairs the firm's privacy and cybersecurity practice. For the past 10 years, he has represented global clients in the financial services, energy, retail, pharmaceutical/health care, cable, telecommunications, car rental, airline, social media, technology, and manufacturing industries, including 35% of Fortune 100-listed companies.

He has represented an array of global clients on privacy and data security projects involving more than 125 countries, and co-founded the International Association of Privacy Professionals (IAPP).

Drawing on his experience and reputation with regulators, Jim also regularly advises companies on compliance practices and through regulatory investigations. His work has included serving as the lead subject matter expert designing security, privacy, and business solutions in several high-profile U.S. Federal Trade Commission (FTC) and U.S. Department of Health and Human Services' Office of Civil Rights (OCR) enforcement proceedings involving social media, mobile, and health care companies.

Prior to joining the firm, Jim led the privacy and cybersecurity practices of two Am Law 100 firms. He also built and led the privacy and co-led the cybersecurity practices at PricewaterhouseCoopers and Booz Allen.

Not any less important than the foregoing, when Jim was 10, he was a Florida State Pixie bowling champion.

Upcoming Webinars and Events

- **Financial Institutions — Are You Ready? An Overview of Breach Threats, Notification Requirements, and Litigation Risks | Thursday, May 19, 2022 | 3 – 4 p.m. ET**

  Financial institutions of all sizes need to know about and prepare for the breach-related threats. Constantly evolving legal requirements and obligations to notify regulators and customers of security incidents also pose compliance challenges, including a new notification requirement for banks that became effective May 1. With the increase of litigation and enforcement actions following cybersecurity incidents, these actions can provide valuable insights, as well as cautionary tales, for financial institutions.

  To learn more, join Troutman Pepper attorneys Kim Phan, Mary Zinsner, and Robyn Lin for a discussion on ways to make sure your organization is ready. Click here to register.

Recent Troutman Pepper Publications

- SEC Reveals Internal Security Incident
- The Clash of Two Movements

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management