Articles + Publications | October 2022

# More Privacy, Please – October 2022

**WRITTEN BY**

Molly S. DiRago | Ronald Raether, Jr. | Gerar Mazarakis | Jenny P. Ji | James Koenig | Robyn W. Lin | Alexandria Pritchett | Lissette Payne | Jack Altura

**Authors:**
Molly S. DiRago
Robyn W. Lin
Lissette Payne
Gerar Mazarakis
Jenny Ji*
Jack Altura
Alexandria Pritchett
Ronald I. Raether Jr.
James Koenig

**Jenny Ji is not licensed to practice law in any jurisdiction; application pending for admission to the California Bar.*

***Editor's Note:*** *In the U.S. laws and regulation space, the White House is focusing on privacy, evident through its session on accountability for big tech and the recent executive order highlighting cybersecurity risks. Meanwhile, the governor of California signed into law the Age-Appropriate Design Code Act and the New York legislature is considering a similar bill titled the Child Data Privacy and Protection Act. In U.S. litigation, a former security chief was convicted of obstructing justice in relation to a data breach, VPPA lawsuits have surged, and major banks have settled with the U.S. Securities and Exchange Commission and Commodity Futures Trading Commission to pay more than $1.1 billion in penalties for violating federal law. In international regulation and enforcement, the European Commission presented the Cyber Resilience Act that could result in fines for noncompliance reaching up to 2.5% of a business's annual revenue.*

## US Laws and Regulation

- **Colorado Releases Proposed Regulations.** On September 30, the Colorado Attorney General's Office released proposed Colorado Privacy Act rules. These proposed rules will be published in the Colorado Register and available for comment on October 10. Notably, the draft rules exempt biometric information from the definition of "publicly available information," further clarify bona fide loyalty programs, and add greater detail to unified opt-out mechanism requirements. The Colorado Privacy Act requires the promulgation of rules by July 1, 2023.
- **Executive Order on Implementing EU-U.S. Data Privacy Framework.** On October 7, President Biden signed an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities. The order directs the steps the U.S. will take to implement the European Union-U.S. Data Privacy Framework. This framework was announced earlier this year in March. Specifically, the order adds further safeguards for U.S. signals

intelligence activities, mandates for handling requirements of personal information, requires U.S. Intelligence Community elements to update their policies and procedures, and creates a multilayer mechanism for qualifying individuals to obtain independent and binding review and redress of claims regarding their personal information.

- **White House Holds Session on Accountability for Big Tech.** On September 8, the White House held a session on tech platform accountability. Included was a listening session with experts and practitioners on "the harms that tech platforms cause and the need for greater accountability." The session identified six key areas: competition, privacy, youth mental health, misinformation and disinformation, illegal and abusive conduct, algorithmic discrimination, and lack of transparency. The White House committed to working with Congress and other stakeholders to address the harms.
- **GAO Calls for Increased Privacy.** On September 13, the Government Accountability Office (GAO) published a new consumer data report on the increasing risk to consumer privacy. The report stated that over the past decade, there has been an increasing collection and use of personal information, which raises concerns related to consumer privacy and protection. The report also referenced the lack of a comprehensive federal privacy law governing collection, use, and sale of personal data, and warned that current laws may not apply to new uses of consumer data.
- **GAO Says U.S. Agencies Need Top-Level Privacy Officials.** On September 22, the GAO released a privacy report revealing that U.S. agencies are struggling to implement privacy programs. For all 24 federal agencies surveyed, the lack of a high-level privacy officer to implement these programs was the primary obstacle. Although these federal agencies have senior privacy officials, they are currently tasked with additional, non-privacy focused duties, preventing the agency from fully incorporating privacy into their risk management strategies. The report recommends employing a high-level privacy officer focused solely on privacy issues to ensure privacy requirements are met. Read more about the GAO report here.
- **Executive Order Regarding CFIUS Includes Privacy.** On September 15, President Biden signed an Executive Order regarding the national security review process of the Committee on Foreign Investment in the United States (CFIUS). This process reviews certain transactions involving foreign investment in the United States. The order directs the committee to consider five specific sets of factors: (1) supply chain risk, (2) technological leadership in areas affecting U.S. national security, (3) industry investment trends that may impact U.S. national security, (4) cybersecurity risks that threaten to impair national security, and (5) risks to U.S. citizens' sensitive data. The order does not define sensitive data, but directs the committee to consider whether a covered transaction involves a U.S. business with access to U.S. persons' sensitive data and whether the investor has sought, or has the ability to exploit such information.
- **BBB States SpongeBob App Violates COPPA.** On September 7, the Better Business Bureau's (BBB) children's advertising branch claimed that Tilting Point Media, LLC, violated the Children's Online Privacy Protection Act (COPPA) and the BBB's Self-Regulatory Guidelines for Advertising and for Children's Online Privacy Protection. Specifically, the agency alleged that the app, The SpongeBob: Krusty Cook-Off, failed to secure verifiable parental consent before collecting information on users below the age of 13 and that the lines between advertising and non-advertising content were not blurred. The agency also stated that children's data could easily be tracked across other companies' apps and websites.
- **Governor Newsom Signs Age-Appropriate Design Code Act.** On September 15, Governor Gavin Newsom signed AB 2273 into law. The bill imposes certain data privacy requirements on businesses that provide services or products that a child will likely access. The bill is modeled after a similar statute in the UK. The Act goes into effect on July 1, 2024.
- **New York Child Data Privacy and Protection Act.** On September 23, the New York legislature introduced Senate Bill S9563, which is awaiting review by the Senate Rules Committee. If passed, the bill would enact the "New York Child Data Privacy and Protection Act," an act aimed at preventing the exploitation of children's data. The bill would require data controllers to assess the impact of its products on children and ban certain data collection and targeted advertising.
- **Michigan's Comprehensive Privacy Bill.** On September 28, Michigan senators introduced Senate Bill 1182, which would affect businesses holding data of more than 100,000 consumers or holding data of more than 25,000 consumers while generating 50% gross revenue from data sales. If enacted, the Michigan Personal Data Privacy Act would comprehensively cover privacy issues, such as data sales and targeted advertising, and provide a private right of action in some instances. Read more about the bill here.
- **Senators Urge Privacy Protection Post-*Dobbs*.** On September 14, thirty U.S. Senators signed a letter urging

the Department of Health and Human Services to take immediate action to strengthen education on, and enforcement of, federal health privacy protection. The letter also urged the department to promulgate rules to update the HIPAA Privacy Rules to broadly restrict regulated entities from sharing individuals' reproductive health information.

- **Maryland DOH Has Yet to Implement Parts of Genealogy Act.** Maryland became one of the first states to address privacy concerns related to forensic genetic genealogy, an investigative method that compares DNA from a crime scene against online profiles of Americans whose DNA are available through ancestry research. However, a Baltimore News Station has reported that the Maryland Department of Health is slow to implement the state's genetic privacy legislation and has yet to report the number of times law enforcement used ancestry data for investigations.

## US Litigation and Enforcement

- **Uber Security Chief Convicted of Covering Up 2016 Data Breach.** On October 5, Joe Sullivan, the former chief security officer for Uber, was convicted of obstructing justice by failing to disclose a breach to the Federal Trade Commission. The charges stem from a data breach in 2016, and a nondisclosure agreement Sullivan signed with the hackers. Prosecutors argued this was evidence he participated in a coverup. This conviction highlights the doubts many chief information security officers have about corporate support, emphasizing the need for improved governance and collaboration with general counsels.
- **Illinois Justices Hear BIPA Time Limit Arguments.** On September 21, the Illinois Supreme Court listened to arguments in *Tims et al. v. Black Horse Carriers Inc.* The Illinois justices heard arguments urging the court to set uniform time limits for bringing claims under Illinois Biometric Information Privacy Act (BIPA). The lower court had ruled that claims brought under Section 15(c) of BIPA are governed by a one-year limit, whereas claims brought under Sections 15(a), (b), and (e) are governed by the statute's five-year limit.
- **Video Privacy Protection Act Lawsuits Surge.** There has been a recent surge in Video Privacy Protection Act (VPPA) lawsuits against companies that offer videos on their websites that use common adtech data tools. VPPA was enacted in 1988, and courts have begun grappling with applying the act to more modern applications, such as streaming services. Among other things, courts have considered the definition of personally identifiable information, and the definition of consumer, and these varying definitions have led to circuit splits.
- **Meta Accused of Working Around Apple's Privacy Restrictions.** On September 15, a new putative class action accused Meta of creating a JavaScript code allowing the platform to work around Apple iOS privacy restrictions to track and store users' online activity and communications. The suit alleges that this code enables the company to intercept, monitor, and record users' personally identifiable information, private health details, text messages, and other information. The suit brings claims under the Wiretap Act, California's Invasion of Privacy Act, and California's Unfair Competition Law, and common law claims of invasion of privacy and unjust enrichment.
- **California Supreme Court Hears Arguments on Scope of Right to Privacy and TCPA.** On September 6, the California Supreme Court heard oral arguments in *Yahoo! v. National Union Fire Insurance Co*. The case concerns whether National Union's insurance policy requiring it to defend claims alleging personal injury, provides coverage in cases alleging a violation of the Telephone Communication Protection Act (TCPA). A lower court held that personal injury coverage only included the right to secrecy and that National Union had no obligation to defend Yahoo. Yahoo is encouraging the court to hold that the right to privacy includes the right to seclusion, which is at the heart of TCPA claims.
- **Major Banks Agree to Pay More Than $1.1B in Fines.** On September 27, Bloomberg reported that major Wall Street banks have agreed to settle with the U.S. Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) and pay more than $1.1 billion in penalties for violating recordkeeping requirements. This settlement arises out of the use of unapproved messaging apps that enabled workers to engage in off-the-record communications, which runs afoul of federal record keeping laws.

## International Regulation and Enforcement

- **Europe Introduces Sweeping Cybersecurity Requirements for Hardware and Software Products.** On September 15, the European Commission presented EU-wide legislation mandating cybersecurity requirements for software and hardware products called the Cyber Resilience Act (CRA), which includes fines for noncompliance reaching up to 2.5% of a business's annual revenue. The act applies to any digital product connected directly or indirectly to another device or network, including wireless and wired devices and software, covers the product's lifecycle, and requires manufacturers to provide security support and software updates to address identified vulnerabilities. Exceptions exist for certain products whose cybersecurity requirements are already established by existing EU rules, including medical devices, vehicles, aviation, and software as a service. The act aims to ensure that businesses will only need to comply with a single set of cybersecurity rules across the EU and must undergo analysis by the European Parliament and Council before its adoption.
- **The Second Biggest Fine Levied Against Instagram for Processing Children's Data in Violation of GDPR.** On September 15, the Irish Data Protection Authority (IDPA) issued a €405 million fine against Instagram (Meta Platforms Ireland Limited (Meta IE)), the second biggest fine levied under General Data Protection Regulation (GDPR). The IDPA complaint focused on the application's processing of children's data, specifically regarding children using personal accounts with default settings set to "public" rather than "private," and the public disclosure of children's contact information, such as email address and/or phone numbers, associated with children using the business account setting. The IDPA employed the dispute resolution mechanism of requesting the European Data Protection Board (EDPB) to resolve other data protection authorities' input on the IDPA decision and penalty. The EDPB found that Meta IE could not rely on Article 6(1)(f) legitimate interests or (6)(1)(b) in performance of a contract as the legal basis of processing.
- **Indonesia Parliament Passes Comprehensive Privacy Law.** On September 20, Indonesia passed comprehensive privacy legislation modeled on the EU GDPR. This law allows for fines of up to 2% of a company's annual revenue, as well as jail time for the falsification of personal data for personal gain or the illegal collection of personal data. The president of Indonesia may form an oversight body to investigate and levy fines against data handlers for violations of the legislation relating to collection and processing of personal data. Notably, data subjects are entitled to financial compensation for data breaches.

## Troutman Pepper Team Spotlight: Joel Lutz

Joel is a privacy and data protection attorney with extensive experience designing and implementing global privacy programs, including 19 years of in-house and law firm experience. He focuses on providing privacy, data security, and commercial advice to technology, financial services, media, ad tech, and health care companies. He has experience developing, implementing, and advising on global privacy programs.

Joel also assists clients with technology licensing, negotiating business agreements, and providing business lines with integrated legal advice from teams of in-house and outside counsel. He leads privacy and security assessments addressing global regulatory compliance and data risk management, including assessments covering: GDPR, CCPA, HIPAA, and FTC Consent Order compliance.

Additionally, Joel advises clients with respect to privacy and security due diligence for mergers and acquisitions. He is also a Certified Information Privacy Professional, representing an array of clients, including the largest technology companies and early-stage companies across industries such as fintech, retail, health care, mass media, social media, manufacturing, biotech, and retail. Joel also served as contributing editor to IAPP's Privacy by Design Core training course.

Joel is a certified barbeque judge by the Kansas City Barbecue Society.

## Upcoming Webinars + Events

- Sadia Mirza (Speaker), "To Notify or Not to Notify: That is the Question," NetDiligence, Santa Monica, CA, October 10, 2022.
- Sadia Mirza (Speaker), "Mother Knows Best – Fireside Chat w/the Moms Leading Privacy, Risk & Security," IAPP P.S.R., Austin, TX, October 14, 2022.
- 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.
- Sadia Mirza (Speaker), "A 'Reasonable' Approach to Data Security," Privacy + Security Forum, Washington, D.C., November 3, 2022.

---

## Recent Troutman Pepper Regulations

- Beware of Goblins, Ghouls, and Phishing Scams – Cybersecurity Awareness Month
- California Age-Appropriate Design Code Is Not Child's Play – Five Practical Tips to Comply and Protect Kids' Privacy
- Four Strategies for Drafting Effective Consumer Breach Notices
- Deadline for New UK Contract Requirements for Personal Data Transfers Is Here (EU and California Deadlines Looming)!
- California AG Sends Letters to Hospital CEOs on Use of Artificial Intelligence

## RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management