

## More Privacy, Please – November/December 2023

### WRITTEN BY

Molly S. DiRago | Ronald I. Raether Jr. | Kim Phan | James Koenig | Natasha E. Halloran | Safvet T. Besen  
| Robyn W. Lin

---

**Editor's Note:** In recent regulatory and enforcement developments, the California Privacy Protection Agency (CPPA) proposed a regulatory framework for automated decision-making technology (ADMT) and revisions to the California Consumer Privacy Act (CCPA) regulations. The Federal Communications Commission (FCC) adopted rules to protect consumers from SIM-swapping scams and port-out fraud, and is investigating the impact of AI on robocalls and robotexts. The FCC plans to expand its data breach reporting rules, while the Federal Trade Commission (FTC) approved the use of compulsory process in nonpublic investigations for AI-related products and services. In litigation, a class action lawsuit was filed against Northwestern Mutual for alleged violation of the Illinois Genetic Information Privacy Act (GIPA), a growing sourcing of litigation for Illinois plaintiffs, and the FTC's privacy complaint against mobile data broker Kochava has been unsealed. Law firm Warner Norcross + Judd LLP has been granted permission to appeal a standing issue related to a ransomware attack, and the Ninth Circuit has restricted the scope of personal jurisdiction applicable to e-commerce platforms and sided with car manufacturers in a privacy claim. Internationally, the EU is establishing a European Health Data Space (EHDS), the UK government proposed amendments to the Data Protection and Digital Information Bill, and the G7 countries signed a code of conduct for AI development.

---

### U.S. Laws and Regulation

**New Jersey Comprehensive Privacy Bill Awaits Governor's Signature.** On January 8, the New Jersey Assembly passed [Senate Bill 322](#). The bill would apply to businesses that control or process the personal data of at least 100,000 consumers, or control or process data of at least 25,000 consumers and derive revenue from the sale of personal data. Consumers would have the right to access, delete, correct, and opt out of the sale of their personal data or the use of their personal information for purposes of targeted advertising or profiling. The attorney general (AG) would have sole enforcement and the director of the Division of Consumer Affairs in the Department of Law and Public Safety would be tasked with promulgating rules and regulations. If signed by the governor, the bill will take effect a year after signing.

**CPPA Proposes Automated Decision Making Technology Framework.** On November 27, 2023, the California Privacy Protection Agency (CPPA) [released their draft](#) for an automated decision making technology (ADMT) regulatory framework. The draft addresses one of the required rulemakings imposed on the CPPA by the California Privacy Rights Act of 2020. The framework discusses the consumers' right to opt out of ADMT and providing more transparency about the businesses' intended use of ADMT. According to the CPPA, these proposed regulations are intended to allow consumers to have control over their sensitive personal information while ensuring that privacy is at the forefront of the design and use of ADMT, including those made by artificial intelligence (AI). The CPPA expects to begin formal rulemaking later in 2024.

**FCC Adopts Rules to Protect Against SIM-Swapping and Port-Out Scams.** The Federal Communications Commission (FCC) [adopted rules](#) in November 2023 to protect consumers from Subscriber Identity Module (SIM) swapping scams and port-out fraud. These scams are carried out by covertly swapping SIM cards from the consumer's phone to a new device or by porting phone numbers to a new carrier without ever gaining physical control of a consumer's phone. According to the FCC, these updated rules set out baseline requirements that establish a uniform framework across the industry while still allowing for flexibility to deliver the best protective measures available. These rules require wireless providers to adopt secure authentication methods for phone number and device swaps as well as immediately notifying the customer whenever a SIM change or port-out request is made. The FCC wants the focus of any wireless provider policy to be protecting consumers' data from privacy threats.

**Colorado AG Publishes Universal Opt-Out Mechanism Shortlist.** On December 28, 2023, the Colorado AG [announced](#) the sole qualifying universal opt-out mechanism (UOOM): the Global Privacy Control (GPC). Beginning on July 1, organizations subject to the Colorado Privacy Act (CPA) must allow consumers to opt out of the sale of their personal data or use of their personal data for targeted advertising using a qualifying UOOM.

**FCC Votes to Investigate AI's Impact on Robocalls and Robotexts.** On November 15, 2023, the FCC [voted 5-0 to pursue an inquiry](#) into the impact of AI on robocalls and robotexts. Chair Jessica Rosenworcel raised concerns about voice cloning scams that test "our ability to separate vocal fact from fiction in order to commit fraud." This comes after a White House executive order called on the FCC to do more to combat AI-facilitated robocalls and robotexts. Members of the Senate Commerce, Science and Transportation Subcommittee on Communications, Media and Broadband likewise recently stated that the FCC was not doing enough to protect consumers. The FCC will soon begin its information-gathering process on the topic, as well as seek comment on how to define AI within this context and assess how AI will affect consumer privacy rights to ultimately determine whether it will pursue additional steps.

**FCC to Expand Data Breach Reporting Requirements.** On November 22, 2023, the FCC [announced](#) that, in response to the evolving and increased frequency and severity of data breaches, it intends to expand and strengthen its existing data breach reporting rules. Specifically, it intends to better align the FCC, federal, and state data breach reporting requirements. The proposed changes to the FCC reporting rules include: (1) expanding the scope to cover all personally identifiable information; (2) expanding the definition of "breach" to include inadvertent access, use, or disclosure of customer information; (3) requiring data breach reports to the FCC in a timely manner; (4) eliminating the notification requirement when reasonably determined harm to customers is unlikely; and (5) eliminating the mandatory waiting period before notifying customers.

**FTC Approves Compulsory Process in AI Products and Services.** On November 21, 2023, the Federal Trade Commission (FTC) [approved an omnibus resolution](#) authorizing the use of compulsory process by the FTC in nonpublic investigations for products and services that use or claim to be produced by AI or the ability to detect its use. The FTC acknowledged that AI offers many beneficial issues, but the FTC cautions that it can be used to engage in fraud, deception, infringements on privacy, and other unfair practices that may violate the FTC Act and other relevant laws. The resolution will streamline the FTC staff's ability to issue civil investigative demands (CID), a process similar to a subpoena, through which the FTC can obtain documents, testimony, and other information relating to AI. The resolution still allows for the FTC to retain its authority to determine when CIDs are issued. The omnibus resolution will be in effect for 10 years.

**FBI Explains Process for How Companies Can Delay SEC Cyberattack Disclosure Requests.** On December 6, 2023, the Federal Bureau of Investigation (FBI) published new guidance on how companies can request a delay in disclosing cyber-attacks to the Securities and Exchange Commission (SEC). Companies must report such attacks to the SEC in Form 8-K filings within four business days unless it is determined that the disclosure would threaten public safety or national security. A delay of public filing for 30 business days can be granted with an option to delay for an additional 30 business days. In extraordinary national security risk circumstances, the deadline can be extended by another 60 business days, provided it does not exceed 120 business days (without an exemptive order from the SEC). These rules took effect on December 18, 2023, however, smaller companies will have an extra 180 days to comply. The FBI recommends that “all publicly traded companies establish a relationship with the cyber squad at their local FBI field office.”

**FTC Proposes Changes to COPPA to Limit Ability to Monetize Children’s Data.** On December 20, 2023, the FTC [proposed changes](#) to the Children’s Online Privacy Protection Act (COPPA) Rule designed to “respond to changes in technology and online practices, and where appropriate, to clarify and streamline the Rule.” The intent is to shift the burden of ensuring that digital services are safe and secure for children from the parents to the providers. FTC Chair Lina M. Khan said, “Kids must be able to play and learn online without being endlessly tracked by companies looking to hoard and monetize their personal data.” The FTC now seeks public comment on its proposed changes to the COPPA Rule.

---

## U.S. Litigation and Enforcement

**Illinois Class Action Lawsuit Filed for GIPA Violation.** On November 8, 2023, a new [class action lawsuit](#) against Northwestern Mutual Life Insurance Company was filed in Illinois. The lawsuit claims that the company violated the Illinois Genetic Information Privacy Act (GIPA) by wrongfully requiring applicants to share information about the medical histories of their family, which the plaintiffs contend is “genetic information” protected by GIPA. The lawsuit contends that the Illinois General Assembly enacted GIPA recognizing the sensitive nature and potential discrimination in the use of such genetic information. The plaintiffs now seek certification of their class action lawsuit and damages of \$2,500 to \$15,000 per alleged violation, plus interest, attorneys’ fees, court costs, and other relief.

**FTC Amends Complaint Against Data Broker Kochava.** On November 3, 2023, the FTC’s privacy complaint against mobile data broker Kochava was unsealed. The [complaint](#) alleges that location data sold by Kochava was “not anonymized” and was “linked or easily linkable” to its consumers. The FTC cited the company’s marketing materials that “emphasize its ability to connect each individual consumer to multiple ‘data points’ in order to ensure that its customers are able to continuously track consumers and connect consumers’ activities with historic and new data.” Kochava argued this amended complaint should remain sealed and sought sanctions against the FTC. However, U.S. District Court Judge B. Lynn Winmill ordered the complaint to be publicly released and rejected the company’s request for sanctions.

**Judge Rules Firm Can Take Data Breach Standing Question to Sixth Circuit.** On November 29, 2023, U.S. District Judge Paul L. Maloney [granted permission](#) for law firm Warner Norcross + Judd LLP to appeal a standing issue to the Sixth Circuit after Judge Maloney allowed a proposed class action to move forward on a negligence claim. This comes after a Michigan federal judge ruled that those whose data was a part of the ransomware attack on the firm’s network have standing to sue based on the heightened risk of identity theft. The standing issue is

key to the outcome of the suit and as such, the proposed class action will be stayed while Warner Norcross + Judd LLP appeals the matter.

**Ninth Circuit Restricts the Scope of Personal Jurisdiction Applicable to E-Commerce Platforms.** On November 28, 2023, the Ninth Circuit [affirmed the district court's dismissal](#) of a putative class action due to lack of specific personal jurisdiction over the defendants. The plaintiff alleged that Shopify, Inc. violated various California privacy and unfair competition laws by deliberately concealing its involvement in certain consumer transactions. The Ninth Circuit held that when a company operates a nationally available e-commerce payment platform and is indifferent to the location of its end-users, the extraction and retention of consumer data, without more, does not subject the defendant to specific jurisdiction in the forum where the online purchase was made. For a deeper analysis by Troutman Pepper, click [here](#).

**TikTok and Users Win Preliminary Injunction Against Montana Bill.** On November 28, 2023, a federal judge granted TikTok and its users' motions for preliminary injunction to block a new Montana law that would ban the social media application within the state's borders. Plaintiffs argued that the statute oversteps state power and could infringe on their First Amendment rights. The judge agreed, noting that "SB 419 bans TikTok outright and, in doing so, it limits constitutionally protected First Amendment speech. Accordingly, SB 419 must pass at least intermediate scrutiny review. Plaintiffs have demonstrated that it is unlikely the law will be able to do so." The judge further noted that "the current record leaves little doubt that Montana's legislature and attorney general were more interested in targeting China's ostensible role in TikTok than with protecting Montana consumers."

**Ninth Circuit Sides With Car Companies in Privacy Battle.** Through a series of rulings, the Ninth Circuit has sided with car manufacturers against claims that the manufacturers violated a [Washington state wiretap law](#) by allegedly intercepting and recording text messages from cellphones connected to on-board infotainment systems. The Ninth Circuit dismissed the claims in four nearly identical opinions, holding that plaintiffs had not shown the requisite injury under the statute. Despite these wins, car manufacturers have faced increased scrutiny for their privacy practices in recent years. In fact, the CPPA [stated](#) earlier this year that they planned to review the privacy practices of "connected vehicle" manufacturers.

**California AG Defends Age-Appropriate Design Code Act.** On December 13, 2023, California AG Rob Bonta [filed a brief](#) in the Ninth Circuit to overturn a district court decision granting a preliminary injunction enjoining the California Age-Appropriate Design Code Act (ADCA) from going into effect. The ADCA is considered a first-in-the-nation law to safeguard children online. The act requires businesses that offer products, services, and features likely to be accessed by children to protect such information and prohibit the collection and use of that information. Bonta says that California will "continue to fight to protect our kids from those who seek to exploit their childhood experiences for profit."

**Insurance Company to Pay \$1M Cybersecurity Penalty to NY DFS.** On November 28, 2023, the New York State Department of Financial Services (NYDFS) [announced](#) that First American Title Insurance Company will pay \$1 million for violations of cybersecurity regulations stemming from the company's 2019 data breach. The NYDFS investigation found that First American "failed to maintain effective governance and classification, access controls and identity management, and risk assessment policies and procedures." This meant that there were insufficient controls in place to prevent hackers from gaining access to the information of First American's consumers.

**Utah Faces Lawsuit Over Social Media Regulations for Children.** On December 18, 2023, a [new lawsuit claimed](#) that Utah's social media regulations unconstitutionally restricted the ability of minors and adults to access content in violation of the First Amendment, the Fourteenth Amendment, and federal law. Under the Utah Social Media Regulation Act, starting on March 1, parents must give permission for a minor to open a social media account and the platforms must verify the ages of all users to open an account. Additionally, the state has mandated a social media curfew that restricts minors' use of social media between 10:30 p.m. and 6:30 a.m. unless authorized by a parent. Utah politicians remain undaunted as they vow to continue their efforts to protect children. The governor included nearly \$1 million to defend the act as part of his 2024 budget proposal.

---

## International Regulation and Enforcement

**EU Seeks to Establish European Health Data Space.** The Environment and Civil Liberties committees [adopted their position](#) on creating a European Health Data Space (EHDS). The EHDS would establish national health data access services monitored by national market surveillance authorities. The intent is to empower citizens to control their personal health care data and facilitate secure sharing for health-related public interests and not-for-profit purposes like research, innovation, education, policy-making, or patient safety and regulatory purposes. The draft position will be voted on by the European Parliament in December.

**Amendments to Data Protection Bill Proposed to UK GDPR.** The UK government has [proposed amendments](#) to the Data Protection and Digital Information Bill, which are described as a "raft of common-sense changes" to build an innovative data protection regime in the UK, crack down on benefit fraud, and allow for new economic opportunities of at least £4 billion. The focus is to make it easier to use personal data to enhance efficiency, improve public services, and enable new innovations across science and technology. The bill was considered and passed through the House of Commons and is now in the committee stage of the House of Lords, one of the final phases in UK's lawmaking process. If passed, it could become law by spring at the earliest.

**G7 Countries Sign Onto AI Code of Conduct.** The G7 countries signed a code of conduct for companies developing artificial technologies. The [announced](#) code of conduct is one of the four pillars of the Hiroshima AI Process Comprehensive Policy Framework which consists of: (1) analysis of priority risks, challenges, and opportunities of generative AI; (2) the Hiroshima Process International Guiding Principles; (3) the Hiroshima Process International Code of Conduct; and (4) project-based cooperation in support of the development of responsible AI tools and best practices. The code of conduct contains 11 guiding principles that "provide guidance for organizations developing, deploying and using advanced AI systems." The G7's stated end-goal of the joint effort is to have an open and enabling environment to safely and securely maximize the benefits and mitigate the risks of AI technology.

**India Proposes Dark Pattern Guidelines.** The India Department of Consumer Affairs [issued proposed guidelines](#) to prevent deceptive marketing tactics or "dark patterns." The Guidelines on Prevention and Regulation of Dark Patterns focus on preventing consumers from being targeted by companies. The guidelines note specified dark patterns, including false urgency, basket sneaking, confirm shaming, forced action, subscription trap, interface interference, bait and switch, drip pricing, disguised advertisement, and nagging.

**ICO Publishes Cookie Compliance Letter for Top Websites.** The UK ICO released a letter the office had sent out in November 2023 to the UK's top-100-most-visited websites, notifying them that their cookie banners may not

be compliant with the Privacy and Electronic Communications Regulations set out by the UK General Data Protection Regulation (GDPR). Resulting from an assessment carried out by the ICO, the letters detail how these websites can address and avoid these errors. The ICO hopes that posting the letter will help other websites comply with the regulations.

---

### **Troutman Pepper Earns Global Rankings in *Chambers Fintech Guide 2024***

Troutman Pepper has once again been ranked among the top law firms globally in the [Chambers FinTech Guide 2024](#) released in December. Both the firm and Partner [Kim Phan](#) continue to be recognized as leading practitioners in the area of Data Protection and Cyber Security. *Chambers FinTech* rankings are based on thousands of thorough research interviews, all conducted by *Chambers'* independent research team. As one respondent noted, "Troutman [Pepper] has had expertise in every question we've asked over the last three years. They are our go-to firm." Another added, "They are able to handle complex matters of significant organizational impact. They have folks spanning many different subject matter expertise and practices such that it can often be a one-stop shop."

---

### **Troutman Pepper Team Spotlight: Kim Phan**

Kim is a partner in the firm's Privacy + Cyber Practice Group, based in our Washington, D.C. office. She counsels companies in federal and state privacy and data security statutes and regulations.

Her work encompasses strategic planning and guidance for companies to incorporate privacy and data security considerations throughout product development, marketing, and implementation. She also assists companies with data breach prevention and response, including establishing effective security programs prior to a data breach and the assessment of breach response obligations following a breach.

Kim also focuses her practice on providing guidance to clients on regulatory compliance matters, including

supervisory and enforcement interactions with the Consumer Financial Protection Bureau (CFPB), the Federal Trade Commission (FTC), and other federal regulatory agencies. She has successfully represented multiple national companies through the FTC investigatory process, resulting in “no-action” letters. She has also counseled a national consumer reporting agency through its CFPB compliance obligations, including conducting risk assessments of consumer products and services, updating policies and procedures, and establishing an audit process to assess compliance with federal consumer financial laws. She frequently writes and speaks about privacy and data security issues for a variety of industries, including consumer financial services, retail, hospitality, higher education, and utilities.

Kim was born and raised in Charlottesville, VA where her mom still lives in the house where she grew up and her two sisters are raising their families. Aunt Kim frequently appears with elaborate gifts for her nieces and nephews, such as an indoor bounce house and backyard zipline, to the chagrin of her sisters.

### Past Webinars, Podcasts, and Events

- Jim Koenig (Speaker), [“Will Generative AI, Including ChatGPT, Transform Businesses, Including Law Firms?”](#) PLI Get Fluent in Technology Seminar, November 13, 2023.
- Kim Phan, Chris Willis (Speakers), [“The NYDFS Updates its Stringent Cybersecurity Regulations. Is This a Bellweather of Coming Industry Change?”](#) Troutman Pepper Consumer Finance Podcast, November 16, 2023.
- Sadia Mirza (Speaker), [Unauthorized Access Podcast: “Ross Is Boss”](#), Troutman Pepper, January 10, 2024.
- Kim Phan, Alison Grounds, Tracey Diamond (Speakers), [“Navigating the AI Revolution – Crafting Effective Policies for Generative AI,”](#) Association of Corporate Counsel (ACC) Greater Philadelphia Chapter — Women’s Summit, November 14, 2023.
- Kim Phan (Speaker), [“AI and Affordable Housing: A National Symposium,”](#) National Council on State Housing Agencies, December 13, 2023.
- Laura Hamady (Moderator), [“Navigating State Privacy Compliance,”](#) Corporate Counsel Institute of the Georgia Bar Association, December 14, 2023.
- Ashley Taylor, Kim Phan, Kristen Eastman, Chris Willis (Speakers), [Exploring the Future of Open Banking: A Discussion on CFPB’s 1033 Proposed Rule – Crossover Episode With Regulatory Oversight Podcast](#), Troutman Pepper, December 14, 2023.
- Kim Phan (Speaker), [“Updating Your Data Breach Investigations and Vendor Oversight to Get Ready for the FTC’s New Breach Notice Amendment to the Safeguards Rule,”](#) Accounts Recovery Webinar, December 15, 2023.
- Robyn Lin, Karla Ballesteros, Natasha Halloran (Speakers), [“Navigating the Complex Landscape of Privacy and Cybersecurity: Emerging Trends, Regulatory Complexities, and Compliance Strategies,”](#) myLawCLE Webinar, January 9, 2024.

---

## Recent Troutman Pepper Publications

- [Navigating the Complexities of Regulatory Data Incident Investigations](#)
- [Trans Union Settles for \\$15 Million with CFPB and FTC Over Tenant Screening Reports](#)
- [Online Tracking Case Dismissed by Ninth Circuit Holding That Online Purchase Does Not Subject Web-Based Payment Processing Platform to Personal Jurisdiction in California](#)
- [FTC Amends Safeguards Rule to Require Reporting of Data Breaches](#)
- [California Takes an Aggressive Approach to Regulating Data Brokers](#)
- [California Delete Act: An Aggressive Approach to Regulating Data Brokers](#)
- [Your Organization has Suffered a Data Incident: Now Here Are the Regulators It Will Likely Encounter](#)

---

Interested in comprehensive legislative and regulatory tracking services focused on consumer financial services? Troutman Pepper offers weekly reports on developments in consumer collection, consumer reporting/FCRA case law, and privacy and data security. Contact Stefanie Jackman ([stefanie.jackman@troutman.com](mailto:stefanie.jackman@troutman.com)), Kim Phan ([kim.phan@troutman.com](mailto:kim.phan@troutman.com)), or Michael Bevel ([michael.bevel@troutman.com](mailto:michael.bevel@troutman.com)) for more information and to request a free trial.

---

Safvet Besen is an associate with Troutman Pepper who is not licensed to practice law in any jurisdiction; application pending for admission to the California Bar.

## RELATED INDUSTRIES + PRACTICES

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