Articles + Publications | December 2022

More Privacy, Please – December 2022

WRITTEN BY

Molly S. DiRago | Ronald I. Raether Jr. | Christopher J. Capurso | Kim Phan | James Koenig | Natasha E. Halloran | Angelo A. Stio III | Alexandria Pritchett | Robyn W. Lin

Editor's Note: *In regulatory news, the Federal Trade Commission extended the deadline to comply with the Safeguards Rule, and Health and Human Services issued guidance for the use of online tracking technology under HIPAA. In U.S. litigation, an Illinois court ruled that a university was exempt under BIPA's GLBA exemption, and the Supreme Court of California held that TCPA insurance may cover right-to-seclusion torts. In international news, the ICO issued guidance on international data transfers, and the Irish DPC imposed additional fines on Meta.*

US Laws and Regulation

- **FTC Extends Deadline for Safeguards Rule Compliance.** The Federal Trade Commission (FTC) extended the deadline for financial institutions regulated by the Gramm-Leach-Bliley Act (GLBA) to comply with certain provisions of its final rule, implementing changes to the Standards for Safeguarding Customer Information (Safeguards Rule) to June 9, 2023. As we previously posted, while certain change provisions to the final rule went into effect earlier this year, other provisions were set to go into effect on December 9. Some provisions affected by the recent extension include, *inter alia*, requirements to designate a qualified individual to oversee an affected entity's information security program and to develop a written risk assessment. The FTC extended the deadline, in part, based on an August 5 letter from the Small Business Administration (SBA) in which the SBA noted the shortage of qualified personnel to implement information security programs and supply chain issues that may lead to delays in obtaining necessary equipment for upgrading security systems.

- **HHS Issues HIPAA Requirements for Online Tracking Technology.** On December 1, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights issued a bulletin to highlight the obligations under the Health Insurance Portability and Accountability Act (HIPAA) when using online tracking technologies. These tracking technologies include cookies and pixels, which collect and analyze information about how internet users interact with a regulated entity's website or mobile application. The bulletin also addressed potential impermissible disclosures of electronic protected health information to online technology tracking vendors.

- **State AGs Call for More Privacy Protections.** On November 17, more than 30 state attorneys general signed a letter to the FTC, responding to the August 22 Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security. The letter commended the FTC for undertaking further rulemaking and specifically called out certain categories of consumer information of concern, data brokers, and encouraging data minimization.

US Litigation and Enforcement

- **Pandora Faces BIPA Lawsuit Over Virtual Jewelry Try-On Feature.** Joining the growing number of Illinois' Biometric Information Privacy Act (BIPA) lawsuits filed against companies utilizing virtual "try-on" technology, on November 15, a proposed class-action suit was filed against Pandora. The suit alleged that the jewelry retailer violated BIPA by collecting customers' facial biometric data through an online feature that allows customers to virtually try on jewelry. The biometric data was allegedly collected without first securing the written, informed consent required under BIPA. The complaint also contended that Pandora failed to establish a retention and deletion schedule for the facial biometric data, and it requested statutory damages permitted under BIPA — *i.e.*, $5,000 for each intentional or reckless violation or $1,000 for each negligent violation — and reasonable attorneys' fees and costs.

- ***Estée Lauder* Virtual Makeup Try-On Feature Opinion Shapes BIPA Requirements.** A federal judge granted in part and denied in part Estée Lauder's motion to dismiss a class-action complaint based on lack of personal jurisdiction, presence of an arbitration clause, failure to state a claim, and lack of standing. The plaintiff alleged that Estée Lauder's virtual try-on tool captured users' facial geometry without informing the user how that data was collected, used, or retained in violation of BIPA. The plaintiff also alleged that the company did not publicly provide a written policy, establishing a retention schedule and guidelines for permanently destroying users' biometric data. The motion was denied in part on the grounds that (1) the company purposefully sold cosmetics in Illinois and is therefore subject to its jurisdiction; (2) the plaintiff's allegations that users could access the try-on tool without encountering the website's browsewrap terms and conditions were adequate to call into question the enforceability of the company's arbitration clause at this stage; (3) the plaintiff alleged sufficient facts to infer that the company captured her biometric information; and (4) the plaintiff has standing since her injury is traceable to the company and can be redressed by a decision in her favor. However, the judge dismissed without prejudice the plaintiff's claim that Estée Lauder intentionally or reckless violated BIPA since she did not plead sufficient facts in her complaint to support this assertion.

- **California Justices Permit TCPA Coverage in CGL Policies.** On November 17, the Supreme Court of California held that if coverage aligns with an insured's reasonable expectations, then commercial general liability policies could cover liability for right-of-seclusion violations litigated under the Telephone Consumer Protection Act (TCPA). For background, the National Union Fire Insurance Company of Pittsburgh, PA (National Union) declined to defend or indemnify Yahoo, Inc. in a series of putative class-action lawsuits, alleging that Yahoo's unsolicited text messaging violated the TCPA. Yahoo sued National Union for breach of contract, seeking to obtain coverage. The negotiated insurance policy provided liability coverage for injuries "arising out of … [o]ral or written publication, in any manner, of material that violates a person's right of privacy." The high court held the personal injury coverage provision was ambiguous under the standard rules of contract interpretation. It further found that the disputed policy could trigger an insurer's duty to defend the insured if the alleged TCPA violation amounted to a right-of-seclusion violation under California law.

- **DePaul University Defeats BIPA Lawsuit Relating to Online Proctoring Software**. On November 4, a federal judge dismissed a putative class-action lawsuit against DePaul University for allegedly collecting their students' biometric identifiers without consent via an online test monitoring software called Respondus Monitor. The judge held that the university was exempt from BIPA under the statute's GLBA exemption because the

university participated in the U.S. Department of Education's Federal Student Aid Program. The judge held that as a program participant, DePaul qualified as a "financial institution" subject to the GLBA, which exempted it from BIPA. Judge Gettleman cited several notable sources to support his ruling, including prior FTC and CFPB rulemaking decisions on GLBA and covered entities.

International Regulation and Enforcement

- **Information Commissioner's Office Issues Further Guidance on Transfer Risk Assessments.** On November 17, the U.K. Information Commissioner's Office (ICO) provided further guidance on international data transfers, including a new section on how to approach a transfer risk assessment (TRA). Compared to the European Data Protection Board's guidance, this assessment focused on the potential risks to human rights as opposed to a comparison of data protection laws. The ICO also introduced a TRA tool to guide companies through the TRA process.

- **Irish DPC Fines Facebook in "Data Scraping" Inquiry.** On November 28, the Irish Data Protection Commission (DPC) imposed a €265 million fine on Facebook. The fine was levied after an inquiry into Facebook's compliance with GDPR's obligation to provide privacy "by design and default." DPC's inquiry related to Meta's implementation of appropriate technical and organization measures, including implementing necessary safeguards.

Troutman Pepper Team Spotlight: Chris Willis

Consumer Financial Services Regulatory Partner and Practice Group Co-Leader Chris Willis advises financial services institutions facing state and federal government investigations and examinations, counseling them on compliance issues, including UDAP/UDAAP, credit reporting, debt collection, and fair lending, and defending them in individual and class-action lawsuits brought by consumers and enforcement actions brought by government agencies. Chris also leverages insights from his litigation and enforcement experience to help clients design new products and processes, including machine learning marketing, fraud prevention and underwriting models, product structure, advertising, online application flows, underwriting, and collection and loss mitigation strategies. Chris brings a highly practical approach to his legal advice, informed by balancing a deep understanding of the consumer finance business and the practical priorities of federal and state regulatory agencies.

An avid traveler, Chris has visited every continent on earth, with the last being Europe.

Recent Webinars, Podcasts, and Events

- Kim Phan (Speaker), "2022 Public Company Seminar," Troutman Pepper Webinar, December 8, 2022.
- Sadia Mirza (Speaker), "California Workplace Developments and Preparing for 2023," Troutman Pepper Webinar, December 8, 2022.
- Kim Phan (Speaker), "Data Security as an Element of Vendor Management," RMAI Webinar, December 12, 2022.
- Kamran Salour and Sadia Mirza (Speakers), "What to Do When a Phishing Attack Happens to You," The Consumer Finance Podcast, December 15, 2022.

Recent Troutman Pepper Publications

- A Look at the Consequences of the Uber and Twitter CISO Cases
- CFPB Highlights Purported "Problems with Tenant Background Checks"
- CFPB Warns CRAs and Furnishers of FCRA Liability for Failing to Conduct Proper Investigations
- CFPB Focuses on Junk Fees, Credit Reporting, and COVID-19 Relief Funds in Latest Supervisory Highlights

The below three articles drafted by Troutman Pepper Privacy + Cybersecurity attorneys landed in the firm's top five insights of 2022.

#2. Whose Crypto Is It, Anyway?

#3. A Fresh "Face" of Privacy: 2022 Biometric Laws

#4. State Attorneys General Association Meetings

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management