Articles + Publications | February 2022

More Privacy, Please – February 2022

WRITTEN BY

Molly S. DiRago | Christopher J. Capurso | Ronald I. Raether Jr. | Graham T. Dean | Jonathan "Grady" Howe | Robyn W. Lin | Lissette Payne | John Sample | Kamran Salour

Editor's Note: Organizations continue calling for a comprehensive federal privacy law, and U.S. states continue trying to fill the void by proposing their own such laws. The latest states to do so include Mississippi and Vermont. Meanwhile, the Federal Trade Commission (FTC), state attorneys general, and private litigants continue litigating, using the mélange of privacy laws available to them, including Illinois' Biometric Information Privacy Act (BIPA) and the Telephone Consumer Protection Act (TCPA). In litigation, defendants have seen some successes: A class action against Bonobos arising out of a data breach was dismissed for lack of standing because the plaintiffs could not demonstrate a substantial risk of future identity theft or fraud. eFinancial successfully pled the TCPA safe harbor defense, despite not fully complying with all safe harbor requirements. Internationally, data protection authorities continue to be busy, including by investigating government agencies. Canada's privacy watchdog is investigating its public health agency as to its use of "de-identified" cellphone location data from 33 million mobile devices. Europol, the EU's police agency, must delete its cache of personal data after an EU data protection watchdog found it was unlawfully collected.

US Laws and Regulation

- **GLBA Amendments to Safeguards Rule Become Effective.** On January 10, the FTC final rule, amending the Standards for Safeguarding Customer Information (Safeguards Rule) under the Gramm-Leach-Bliley Act (GLBA), became effective. The amendments add provisions related to, among other things, risk assessments, vendor oversight, and incident response plans. The amendments also expand the definition of "financial institution." Though the final rule became effective on January 10, the compliance date for many of these provisions will begin on December 9. To read more, click here.

- **Introducing the Banning Surveillance Advertising Act.** Congresswomen Anna G. Eshoo (D-CA) and Jan Schakowsky (D-IL) and Senator Cory Booker (D-NJ) introduced the Banning Surveillance Advertising Act, which would prohibit advertising networks and facilitators from using personal data to target advertisements. An exception would exist for broad location targeting to a recognized place, such as a municipality. The bill also would prohibit targeted advertising based on protected class information, such as race, gender, and religion, and personal data purchased from data brokers. To read the press release, click here.

- **US Chamber of Commerce Calls for Federal Privacy Law.** On January 13, the U.S. Chamber of Commerce and local business organizations from 28 states wrote a letter, urging Congress to pass a comprehensive federal privacy law. The letter explains that the emerging patchwork of state laws "take significantly diverse approaches on enforcement, duties, and scope," which "create consumer and business confusion." The letter advocates "that Congress pass one single national standard" that "provide[s] meaningful and robust

protections for consumers through sole federal agency and state attorney general enforcement." The Chamber endorsed Rep. Suzan DelBene's (D-WA) Information Transparency and Personal Data Control Act last year, which included strong preemption language and has been in committee since March 2021.

- **Comprehensive Privacy Bills Introduced in Mississippi and Vermont.** Mississippi and Vermont are the latest states to introduce comprehensive privacy bills similar to the California Consumer Privacy Act (CCPA). Mississippi's Senate Bill 2330 proposes data subject rights, a "do not sell" provision, a private right of action, and attorney general enforcement. The Vermont General Assembly has proposed two comprehensive privacy bills in the House of Representatives. Vermont House Bill 160, carried over from the 2021 legislative session, proposes to adopt consumer privacy protections, give Vermonters more control over the amount and type of data that personal device manufacturers and service providers collect about them, and adopt other protections provided in the CCPA. Vermont House Bill 570, raised at the start of the current session, purports to "enhanc[e] data privacy protections for consumers."

US Litigation and Enforcement

- **Telematics Users Become Next Target of BIPA Litigation Wave.** The newest target for plaintiffs wielding their private right of action under Illinois' BIPA are companies using or offering dash-cam "telematics." Telematics involves use of an in-vehicle camera device that employs artificial intelligence, machine learning, and "computer vision" to collect and analyze, among other things, driver behavior. In January, at least two complaints were filed against companies using and providing telematics services, mirroring similar complaints filed in previous months. Notably, the defendants are not Illinois-based companies. To read more, click here.

- **FTC Settlement Clarifies FCRA and Privacy Requirements for Lead Sales.** On January 7, the FTC announced that it had reached a $1.5 million settlement with ITMedia Solutions LLC and its affiliates. The FTC alleges that ITMedia and its affiliates collected sensitive information from consumers for loan applications after assuring these consumers that it would only share the information with "trusted lenders, lending partners and financial services providers." According to the FTC, the information was actually sold to non-lenders for lead generation purposes, and the representations therefore constituted "deceptive acts or practices in violation of Section 5(a) of the FTC Act." To read more about this settlement, click here.

- **Class-Action Lawsuit Against Bonobos Gets Dismissed.** On January 19, the Southern District of New York dismissed the class-action lawsuit against Bonobos for failing to meet standing requirements. Last year, Bradley Cooper filed a class action against Bonobos, alleging that partial credit card numbers, encrypted passwords, telephone numbers, email addresses, and other personal data were compromised in a data breach and posted onto an online forum used by cybercriminals. The court found that the plaintiff did not make "plausible allegations of misuse" or show a "substantial risk of future identity theft or fraud." The court explained that although Cooper's partial credit card number had been compromised, he had the ability to cancel the card, which would have eliminated any future risk of harm. As to the compromised passwords, they were encrypted, Bonobos reset the passwords, and there were no allegations that the compromised passwords were used on other websites/accounts. Accordingly, the likelihood that harm would result from the exposed data

was too remote to support standing.

- **Defendant Successfully Invokes TCPA Safe Harbor Affirmative Defense.** The Western District of Washington granted summary judgment in favor of eFinancial LLC, adopting the magistrate judge's recommendation in *Johansen v. eFinancial LLC*, No. 2:20-cv-01351. The magistrate found that eFinancial had permission to call the plaintiff, but even if it did not, the TCPA safe harbor defense applied even though eFinancial had not complied fully with safe harbor requirements. Although there was evidence that eFinancial did not maintain an internal do not call (DNC) list and did not purchase and access the National DNC Registry, the court held that eFinancial "substantially complie[d]" with safe harbor requirements and thus could successfully invoke the defense.

- **Ancestry.com Files Response Brief in Class-Action Lawsuit.** Ancestry.com recently filed a response brief in the Ninth Circuit, supporting the Northern District of California's decision (described in our September 2021 *MPP* edition) that held that Ancestry.com was immune under Section 230 of the Communications Decency Act (CDA) for publishing school yearbook photos. Ancestry.com argues that the yearbook photos are third-party content that Ancestry.com merely republished and "like all individuals pictured in yearbooks, Plaintiffs long ago consented to public distribution of these photos without restriction or control." The plaintiffs argue CDA immunity only applies where the yearbook provides the information and consent prior to publication. According to Ancestry.com, requiring prior consent of the original poster would "upend the CDA statutory scheme" and create "incalculable liability" for internet companies.

International Regulation and Enforcement

- **European Data Protection Board Adopts Guidelines on Right of Access.** The European Data Protection Board (EDPA) adopted *Guidelines on Right of Access* during its January plenary session. The guidelines aim to provide clarification on the scope of the right of access, the information a controller must provide to a data subject, the format of the access request, the main modalities for providing access, and the parameters of manifestly unfounded or excessive requests. The guidelines will be subject to public consultation for a period of six weeks. To read the press release, click here.

- **Canadian Privacy Watchdog Investigates Health Officials' Use of Cellphone Data.** The Canadian privacy watchdog is investigating federal officials' use of "de-identified" cellphone location data to analyze trends in "movement of populations" and measure the efficacy of COVID-19 health measures. The Public Health Agency of Canada (PHAC) acknowledged that it purchased the data but stated it could not track individuals because the data was de-identified. PHAC accessed location data from 33 million mobile devices.

- **European Parliament Approves Digital Services Act.** The European Parliament recently approved a draft of the Digital Services Act (DSA), which intends to regulate the obligations of digital services that act as intermediaries in their role of connecting consumers with goods, services, and content. The DSA includes

measures to counter illegal content online, including goods and services; new rules on traceability of business users to help identify sellers of illegal goods; safeguards and transparency measures for users; obligations for very large online platforms to prevent abuse of their systems; and oversight structure to address the complexity of the online space. To read the full press release, click here.

- **European Police Ordered to Delete Personal Data Cache.** The EU's police agency — Europol — will delete a vast store of personal data after an EU data protection watchdog found it to be unlawfully amassed. The data contained billions of points of information, including sensitive data from crime reports and data hacked from encrypted phone services. Europol's cache allegedly contains at least four petabytes of data — equivalent to three million CD-ROMs or a fifth of the U.S. Library of Congress' entire content.

- **Polish DPA Fines Warsaw University of Technology.** After the Warsaw University of Technology suffered a data breach in May 2020, the Polish data protection authority (DPA) investigated and held that the university did not implement the appropriate technical and organizational measures to ensure the security of the personal data processed. The fine totaled PLN 45,000 (approximately EUR 9,900 and $11,200 USD).

- **Italy's DPA Issues €26.5M Fine for GDPR Violations.** After Enel Energia violated the EU General Data Protection Regulation (GDPR), Italy's data protection authority, the Garante, fined the multinational electric and gas distribution €26.5 million. The Garante found that Enel Energia employed "aggressive telemarketing" tactics by unlawfully processing personal data for telemarketing purposes, thereby violating GDPR provisions around accountability and user consent.

Troutman Pepper Team Spotlight: Kamran Salour

Partner Kamran Salour recently joined the Troutman Pepper's Cybersecurity, Information Governance, and Privacy Practice Group in the firm's Orange County office. He dedicates his practice to helping clients reduce the likelihood of experiencing a data security incident, while minimizing the impact in case of a potential occurrence. He focuses his practice on guiding his clients through the incident response process. This process includes directing forensic investigations, developing post-incident response notification plans, and responding to regulatory investigations.

For each data incident, Kamran seeks to answer three main questions for his clients: (1) how the incident occurred; (2) how best to comply with any legal obligations the incident created; and (3) how to reduce the likelihood of an incident happening again. Kamran also helps his clients assert or defend against claims in state and federal litigation, resulting from data security incidents. Apart from incident responses, Kamran further assists clients with pre-incident planning, including developing incident response plans and modifying vendor agreements to clarify each parties' obligations should an incident occur. As a Certified Information Privacy Professional for the U.S. and Europe (CIPP/US/E) and a Certified Privacy Information Technologist (CIPT), Kamran also counsels companies about information governance and helps them comply with data protection laws.

Armed with years of experience as a litigator, Kamran provides his clients with a unique perspective on data privacy and protection issues. He brings a pragmatic problem-solving approach to his incident response work — an approach that he developed and honed through years of resolving high-stakes litigation disputes on behalf of his clients. Using his litigation experience, Kamran leverages his skill set in understanding and anticipating drafting ambiguities and oversights that spawn litigation to his clients' benefit when counseling them on compliance.

In his personal life, Kamran holds the distinction of having the most "late" cancelations at his local Orangetheory fitness studio.

Recent Troutman Pepper Publications

- **Illinois Supreme Court Rules on Workers' Compensation Act and BIPA**
- **Solidifying Security Systems Standards**
- **First Amendment Challenge to Restriction on Public Access to Electronic Court Records Advances**
- **GLBA Safeguards Rule Amendments Become Effective — December 2022 Compliance Countdown for Key Provisions Begins**
- **Drivers' Telematics Violates BIPA**

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management