Articles + Publications | June 2022

More Privacy, Please – June 2022

WRITTEN BY

Molly S. DiRago | Christopher Carlson | Noah J. DiPasquale | Ronald Raether, Jr. | David N. Anthony | Angelo A. Stio, III | Ashley L. Taylor, Jr. | Robyn W. Lin | Lissette Payne | Alexandria Pritchett | Rachel Miklaszewski | Andrew Raunau | Kamran Salour

Authors:
Molly S. DiRago
Robyn Lin
Lisettee Payne
Alexandria Pritchett
Chris Carlson
Rachel Miklazewski
Noah DiPasquale
Andrew Raunau
Ronald I. Raether Jr.
David N. Anthony
Kamran Salour
Angelo A. Stio III
Ashley L. Taylor, Jr.
Safvet Besen*
Justin Stalberg*

Editor's Note: This past month featured increased activity in privacy and data protection. **U.S. Legislation and Regulation.** Connecticut's governor signed a comprehensive privacy bill, and President Biden has before him a bill that would improve information sharing among Tribal, state, and local governments about cybersecurity. The U.S. House of Representatives also passed a bill to support research on privacy-enhancing technologies and promote responsible data use (while the Government Accountability Office (GAO) criticized the Department of Defense's (DOD) component agencies for lack of compliance with cybersecurity policies). **Industry.** Business leaders joined to issue guidance to lawmakers and regulators on artificial intelligence and machine learning, and two federal judges called for further funding to combat cybersecurity threats and enhance courthouse safety. The Federal Trade Commission (FTC) announced further scrutiny of children's educational technology. **U.S. Litigation and Enforcement.** State attorneys general have announced a new Center on Cyber and Technology to enhance the technical capabilities of state AGs. Illinois continues to see privacy litigation, including one against the popular social media application Snapchat, and the Illinois Supreme Court heard oral arguments on the nature of BIPA damages. District courts continue to see class action privacy litigation, including class certifications for classes of consumers who experienced a data breach, and dismissal of another class alleging violation of the Driver's Privacy Protection Act (DPPA). **International Regulation and Enforcement.** Uber was fined €4.24M, the European Data Protection Board released guidelines on calculating GDPR fines, and the Canadian Office of the

Privacy Commissioner has issued an interpretative guideline on the definition of “sensitive information.”

US Laws and Regulation

- **Connecticut Governor Signs Comprehensive Privacy Bill.** On May 10, Connecticut Gov. Ned Lamont signed an act concerning personal data privacy and online monitoring, making Connecticut the fifth state in the country to enact a comprehensive privacy regime. This legislation closely resembles the laws adopted in Virginia and Colorado, and will take effect on July 1, 2023. The Connecticut law does not include a private right of action and provides a temporary 60-day right to cure that sunsets on December 31, 2024. For more information click here.

- **GAO Urges DOD To Do More To Protect Unclassified Information.** Recent reports from the GAO show that none of the DOD’s component agencies are fully compliant with the cybersecurity policies for protecting controlled unclassified information (CUI). On average, the agencies are only 70% compliant with the policies, despite DOD regulations requiring 100% compliance. The DOD’s cybersecurity rules fall into three broad compliance requirements: (1) categorize systems containing CUI accurately and determine whether compromising those systems would have a low, moderate, or high impact on DOD operations; (2) implement specific levels of cybersecurity controls depending on the expected impact of a breach; and (3) determine whether systems that contain CUI have a valid authorization to operate on the DOD’s network and perform periodic risk assessments.

- **Federal Judges Request $8.6B to Combat Cybersecurity Threats and Courthouse Safety.** Two federal judges, Amy J. St. Eve and Roslynn R. Mauskopf, testified that a Judiciary budget of $8.6 billion is needed to keep pace with inflation and to pay for important new investments in courthouse security, IT modernization, and cybersecurity. According to the judges, the investment is needed for functionality purposes, but also to combat cyber threats and protect the safety of courthouses and judges. Judge Mauskopf additionally called for the passage of the Daniel Anderl Judicial Security and Privacy Act of 2021, which would prohibit the distribution of personal information that could put judges and their families at risk.

- **Federal Trade Commission to Tackle Edtech Surveillance of Children.** On May 19, the FTC adopted a new policy statement, announcing a crackdown on education technology companies that surveil children when they go online to learn. The statement warns that edtech providers must comply with the Children’s Online Privacy Protection Act (COPPA). COPPA imposes data minimization requirements, use prohibitions, notice requirements, retention limitations, and security obligations. Companies that fail to follow COPPA could face potential civil penalties and new requirements and limitations on their business practices.

- **New Cybersecurity Legislation Passes House.** On May 17, the State and Local Government Cybersecurity Act of 2021 (S.2520) passed the House, and now awaits President Biden’s signature. The act would update the House Homeland Security Act and direct the Department of Homeland Security to improve information sharing and coordination with state, local, and Tribal governments. It would encourage federal cybersecurity experts to share information regarding cybersecurity threats, vulnerabilities, and breaches, as well as resources to prevent and recover from cyberattacks. The bill would also build on previous efforts by the Multi-State Information Sharing and Analysis Center (MS-ISAC) to prevent, protect, and respond to future cybersecurity incidents.

- **Business Roundtable Issues Guidance to Regulators and Lawmakers on Artificial Intelligence and Machine Learning.** At the start of the year, the Business Roundtable—a group of 230 CEOs from some of the largest companies in the world—developed guidance for policymakers who regulate Artificial Intelligence (AI) and Machine Learning (ML). This guidance aims to strike a balance between providing some governmental oversight while ensuring that new technology and innovation are not unduly curbed. Additionally, the Business Roundtable issued a set of core principles to encourage companies in this space to self-regulate. To read more on these recommendations, click here.

- **Promoting Digital Privacy Technologies Act Passes House.** On May 11, the Promoting Digital Privacy Technologies Act (H.R. 847) passed the House by a vote of 401-19. The act seeks "to support research on privacy-enhancing technologies and promote responsible data use." Notably, this legislation would require the National Institute of Standards and Technology (NIST) director to work with private, public, and academic stakeholders to develop privacy-enhancing technologies and "voluntary, consensus-based technical standards, guidelines, methodologies, procedures, and processes" aimed at increasing the "integration of privacy-enhancing technologies in data collection, sharing, and analytics performed by the public and private sectors." H.R. 847 now heads to the U.S. Senate Committee on Commerce, Science, and Transportation. For more information, click here.

US Litigation and Enforcement

- **NAAG Launches Center on Cyber and Technology.** On May 9, the National Association of Attorneys General (NAAG) announced the creation of the Center on Cyber and Technology (CyTech). CyTech seeks to enhance the technical competency of state AGs and staff by: (1) developing programming and dedicating resources to support the understanding of emerging and evolving technologies; (2) conducting cybercrime investigations and prosecutions: and (3) ensuring secure and resilient public and private sector networks and infrastructure. CyTech will also provide tools and support for state AGs' technology-related enforcement actions. Companies, in-house counsel, and their IT executives should take additional steps to pay attention to CyTech's list of topics to anticipate potential areas of scrutiny and enhance their policies, procedures, and training in those areas.

- **Snap Sued over Photo Filters.** Snap Inc., the parent company of Snapchat, is facing a federal privacy suit accusing the social media giant of violating the Illinois Biometric Information Privacy Act (BIPA). Plaintiffs filed a proposed class action last week, alleging that Snap Inc. failed to obtain permission from users in Illinois before scanning their facial geometrics. Snapchat's popular Lenses feature captures and uses biometric facial data to apply different filters to a user's face. Plaintiffs claim that Snap violated BIPA because it neither informed Illinois users that the company was collecting their private identifying information, nor explained its data collection practices.

- **Illinois Supreme Court Poised to Determine When BIPA Claims Accrue.** On May 17, the Illinois Supreme Court heard oral arguments on when claims accrue under sections 15(b) and 15(d) of BIPA in *Cothron v. White Castle*. Responding to a question certified by the Seventh Circuit, the Illinois Supreme Court will decide whether BIPA claims accrue each time a private entity scans a personal biometric identifier or transmits such a scan to a third party, or whether such claims accrue only upon the first scan or transmission to a third party. The answer to this question is crucial not only for these litigants (if accrual only occurs on the first scan or transmission,

plaintiff's claims are completely time-barred), but for future BIPA litigants as well. BIPA provides for steep statutory penalties "for each violation." Therefore, a ruling that only the first scan or transmission is a "violation" would limit claims and, more importantly, damages recoveries for BIPA plaintiffs going forward. A ruling that each scan or transmission is a "violation" would likely mean exponentially more exposure for future defendants, as damages awards would be multiplied by each scan or transmission.

- **Lemonade Insurance Reaches $4 Million Class Settlement After Alleged BIPA Violations.** Earlier this year, a class of policyholders sued Lemonade Insurance for violating BIPA and similar statutes by improperly collecting and storing plaintiffs' biometric information when they filed insurance claims online. On May 17, plaintiffs filed a motion for preliminary approval of a settlement whereby Lemonade would pay $4 million to its policyholders whose facial data was collected between June 2019 and May 2021. The proposed settlement would allocate $3 million to a subclass of about 5,000 policyholders in Illinois who alleged that Lemonade violated BIPA, and the remaining $1 million would go to a subclass of about 110,000 policyholders in states other than Illinois. The preliminary settlement also requires Lemonade to, among other things: (1) no longer collect customers' biometric information, and, if it decides to do so in the future, comply with BIPA; and (2) destroy all biometric information it collected from class members.

- **District Court Partially Grants Certification of Consumer Data Breach Class Action.** The U.S. District Court for the District of Maryland issued a class certification decision in a multidistrict consumer data breach case against an international hotel company, becoming one of the few district courts to certify a limited Rule 23(b)(3) class in a consumer data breach case. Notably, the court substantially narrowed the classes to eliminate individuals whose claims were dissimilar to the named plaintiffs,' and denied certification of a proposed class of plaintiffs claiming breach of state data breach notification laws and classes requesting injunctive relief. The court held that the limited proposed 23(b)(3) classes were ascertainable, however, because the single database that was exposed in the data breach contained the names and contact information for virtually all of the class members. The court concluded that any gaps could be filled through an objective, "mechanical" review of available additional records. For further analysis of the court's certification decision, click here.

- **District Court Grants Motion to Dismiss Alleging Violations of DPPA.** The U.S. District Court for the Western District of Wisconsin granted the defendants'/insurers' motion to dismiss class action claims that they breached the Driver's Privacy Protection Act (DPPA) by disclosing drivers' license numbers through an "instant quote" feature on their websites. Essentially, hackers with only basic, identifying information were able to prompt the "instant quote" feature to auto-fill other, personal information about that individual, including a person's driver's license number. The court dismissed the matter for lack of Article III standing, finding that plaintiffs' allegation that the data breach resulted in an "increased risk of fraud and identity theft" was not imminent and too speculative. The court emphasized that only drivers' license numbers were disclosed, which are not sensitive forms of data. The decision is being appealed to the Seventh Circuit.

International Regulation and Enforcement

- **Italy Imposes €4.24M in Fines to Uber & Uber Technologies Following Data Breach.** The Italian data protection authority (Garante) announced on May 19 that it would impose a total of €4.24M ($4.54M) in fines to

Uber B.V. and Uber Technologies Inc. for violations of Articles 13, 23, 37, and 38 of Legislative Decree No. 196 of June 2003 and the Personal Data Protection Code. This follows an *ex officio* investigation by the Garante for a data breach involving the data of approximately 57 million users worldwide in 2016. Uber's violations include: (1) providing an information notice to users that was formulated in a generic and approximate manner with unclear and incomplete information (Article 13); (2) failing to obtain valid consent before processing the data of approximately 1.38M passengers by profiling them on the basis of a 'fraud risk' (Article 23); and (3) failing to notify the Garante that it processed data for geolocation purposes (Articles 37 and 38).

- **EDPB Releases Guidelines for Calculating GDPR Fines.** Data protection authorities now have a framework to use when calculating GDPR fines. The European Data Protection Board (EDPB) released a set of guidelines, which includes a five-step process to be used when determining fines: (1) identify the processing operations and application of Article 83(3) of the GDPR; (2) consider a starting point for calculations based on evaluating Chapter 4 of the GDPR; (3) consider any aggravating and mitigating circumstances; (4) identify relevant legal maximums for the processing operations; and (5) consider whether the final amount meets the requirements of effectiveness, dissuasiveness, and proportionality. The guidelines also discuss many other topics relating to fines, such as fixed-amount fines, concurrent infringements, unity of action, previous infringements, and degree of cooperation with supervisory authorities. The EDPB is accepting public comment on the guidelines until June 27, 2022.

- **Office of the Privacy Commissioner of Canada Issues Interpretation Bulletin.** The Office of the Privacy Commission of Canada (OPC) issued an interpretive bulletin around the definition of "sensitive information" under the Personal Information Protection and Electronic Documents Act (PIPEDA). While not a binding legal interpretation, the bulletin provides guidance for compliance with PIPEDA. The bulletin provides examples of information determined to be "sensitive," including in the health and financial sectors. While what information is "sensitive" will vary depending on the facts of each case, information related to health and financial data, ethnic and racial origins, political opinions, genetic and biometric data, an individual's sex life or sexual orientation, and religious or political beliefs is generally considered sensitive.

Troutman Pepper Team Spotlight: Brent Hoard

Brent Hoard recently joined us as a partner. Clients rely on Brent's unique legal and consulting experience to find practical solutions to today's complex and evolving privacy and data protection issues. Brent has helped an array of clients — from Fortune 50 companies to early-stage innovators, across a spectrum of industries — to protect and maximize the value of their data through assessment, development, implementation, and enhancement of their privacy, information security, risk management, and HIPAA programs. These industries include technology, social media, health care, pharmaceuticals and life sciences, digital health, internet, retail, insurance/reinsurance, fintech, and travel/hospitality.

Before the start of his professional career, Brent pitched in the Minnesota Twins organization from 1998 to 2004, and was a member of the Twins' 40-Man Major League Roster in 2003.

**Safvet Besen and Justin Stalberg are 2022 summer associates with Troutman Pepper and not licensed to practice law in any jurisdiction.*

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management