Articles + Publications | July 2021

More Privacy, Please – July 2021

WRITTEN BY

Molly S. DiRago | Ronald Raether, Jr. | David N. Anthony | Angelo A. Stio, III | Ashley L. Taylor, Jr. | Edgar Vargas

Authors:
Molly S. DiRago
Ronald I. Raether Jr.
David N. Anthony
Angelo A. Stio III
Ashley L. Taylor, Jr.
Edgar Vargas
Rachel Goldner*
Camille Sanches*

Do you want a simple way to keep current on important privacy changes? Avoid sleepless nights wondering whether you missed a privacy speed bump or pothole between annual updates? Worry no longer. Troutman Pepper is pleased to offer *More Privacy, Please* — a monthly newsletter recapping significant industry and legal developments, as well as trends in the areas of cybersecurity, information governance, and privacy.

U.S. LAWS AND REGULATION

- **Colorado Passes Comprehensive Privacy Law.** On June 8, the Colorado legislature passed the Colorado Privacy Act (CPA), becoming the third state to enact a comprehensive data privacy law following the California Privacy Rights Act of 2020 (CPRA) and the Virginia Consumer Data Protection Act (VCDPA). While there are differences, the CPA is much like the California Privacy Rights Act of 2020 (CPRA), which amended the California Consumer Privacy Act of 2018 (CCPA), as well as the recently enacted VCDPA. For an overview of the new law, read our latest article here.

- **South Carolina Introduces Innovative Privacy Bill.** South Carolina recently proposed a new biometric privacy bill — the Biometric Data Privacy Act (BDPA) — which stands out from previous bills proposed in New York and Maryland because it adopts additional compliance obligations. Some of the bills' unique features include (1) providing consumers with various rights, such as opt-out, deletion, and anti-discrimination rights, over the collection and use of their biometric data; (2) requiring employee training to ensure proper compliance and handling of consumer inquiries; and (3) permitting businesses to offer financial incentives for the collection, sale, or deletion of biometric information. The BDPA contains a private right of action and steep statutory damages of up to $1,000 for negligent violations and $10,000 for intentional or reckless violations. The BDPA would only apply to businesses in South Carolina but could provide an example for other states as the use of biometric

data increases.

- **Nevada Broadens Privacy Law. On June 2, Nevada's governor approved amendments to NRS 603A.300-360, the state's internet privacy legislation.** This law gives consumers the right to opt out of the sale of their data to third parties and broadens the scope of the law to apply to "data brokers." The changes are expected to go into effect October 1, 2021.

- **Texas Updates Data Breach Notification Law.** On June 14, Texas House Bill 3746 was signed into law, amending the state's data breach notification law (Texas Business and Commerce Code § 521.053). While the statute already requires notification to the Texas attorney general and individuals following certain data breaches, the amendment requires the Texas attorney general to post a list of all data breaches that involve 250 or more Texas residents on its website. California has a similar requirement for data breaches affecting 500 or more residents.

- **Connecticut Enhances Data Breach Notification Law.** Connecticut's attorney general announced the passage of "An Act Concerning Data Privacy Breaches," an enhanced data breach notification law. The new law includes a range of updates to better protect Connecticut residents, such as an expanded definition of "personal information" and additional data categories.

- **Senator Gillibrand Pushes for a US Data Protection Agency.** On June 17, Senator Gillibrand reintroduced the Data Protection Act, which would establish a new, independent agency responsible for policing Big Tech mergers and discriminatory data practices. The new Data Protection Act of 2021 recently gained support from a range of privacy, technology, and civil rights organizations, including the Electronic Privacy Information Center and Public Citizen.

U.S. LITIGATION AND ENFORCEMENT

- **Supreme Court Clarifies 'Concrete Harm' in Data Dissemination Case.** On June 25, the Supreme Court issued its opinion in *TransUnion LLC v. Ramirez*, holding that a concrete injury requires more than the existence of a risk of harm that never materializes. Accordingly, the vast majority of the absent class members, who could not prove that allegedly inaccurate credit reports were disseminated to any third party, did not have Article III standing to assert a claim in federal court under the Fair Credit Reporting Act (FCRA). The opinion has potentially far-reaching implications, well beyond the FCRA. Lower courts will likely debate the contours of the decision in the coming months. To read an in-depth analysis of the opinion, click here.

- **Topgolf Agrees to $2.6 Million Settlement in BIPA Suit.** After private mediation in the spring, Topgolf agreed to pay a $2.6 million settlement to resolve litigation brought by former employees. Ex-Topgolf workers alleged that the company violated Illinois' Biometric Information Protection Act (BIPA) when it collected employees' fingerprint data and distributed the data to its timekeeping vendor without receiving the employees' informed

consent. The settlement could lead to an estimated net recovery of $630 per person for the proposed 2,660-member class. Plaintiffs are now seeking class certification.

- **Eleventh Circuit Approves $1.4 Billion Equifax Class Action Settlement.** On June 3, the Eleventh Circuit upheld the $1.4 billion settlement arising from Equifax's 2017 data breach. The court rejected concerns that the class lacked adequate representatives and that the attorneys' fees $77.5 million award (more than 20% of the settlement fund) should be reevaluated. Critically, the Eleventh Circuit held that the plaintiffs, whose identities were not stolen, still had standing to sue. The court found that the plaintiffs' allegations that they faced a material and substantial risk of identity theft were adequate due to the "colossal amount of sensitive data stolen, including Social Security numbers, names and dates of birth, and the unequivocal damage that can be done with this type of data."

- **Judge Sides with Apple and Denies Motion to Compel Document Production in Privacy Class Action.** On June 16, Chief Nancy Rosenstengel of the Southern District of Illinois denied the plaintiffs' motion to compel the production of certain documents in a privacy case against Apple. The plaintiffs in the putative class action alleged that Apple violated Illinois' BIPA by collecting customers' biometric identifiers, including scans of facial geometry, without obtaining informed consent. The plaintiffs requested documents sufficient to identify every Illinois resident who used Apple devices containing the Photos app since 2016 and documents sufficient to identify all Illinois residents who executed the app's license agreements. Judge Rosenstengel sided with Apple, claiming the requests were far too broad and intrusive and unrelated to class certification. Judge Rosenstengel also expressed concerns regarding the privacy of the requested information, stating, "Plaintiffs have provided the Court with no explanation as to how the data would be stored and kept secure, which is crucial considering the rising number of computer hackings and ransomware attacks hitting U.S. companies."

- **Six Flags Agrees to $36 Million Settlement in Momentous Biometric Privacy Suit.** Six Flags agreed to a $36 million settlement in a class action, which alleged that it collected passholders' biometric fingerprint data without receiving prior informed consent. The class consists of all individuals who visited Six Flags Great Adventure in Gurnee, Illinois between October 1, 2013 and December 31, 2018, and scanned their fingers on a scanner at the park's entry gates. In 2019, the Illinois Supreme Court unanimously ruled that plaintiffs could bring claims for BIPA violations without alleging a separate, real-world harm. You can read more about that decision here.

INTERNATIONAL REGULATION AND ENFORCEMENT

- **European Commission Implements New Privacy Regulations.** On June 4, the European Commission released two sets of standard contractual clauses (SCCs) — one for use between controllers and processors and another for transferring personal data to third countries. The two sets were introduced following new requirements established under the General Data Protection Regulation (GDPR) and *Schrems II* These templates appear to be the European Commission's attempt to assist European Union (EU) legal compliance efforts regarding international data transfers. Troutman Pepper will have additional thoughts on these SCCs by

next week — stay tuned! To read the European Commission's announcement, click here.

- **Italy to Create National Crime Agency to Fight Cyberattacks.** In an attempt to fight cyberattacks, Italy plans to create a unified cloud infrastructure. This decision occurred after several other European countries took steps to improve their defenses against cyber risks. Unlike the current system, which is dispersed among different ministers and state bodies, the new agency will operate under one general director and will include six departments. Part of Italy's recovery plan, the crime agency was sent to the European Commission in April. Currently, U.S. tech companies Google, Microsoft, and Amazon dominate the data storage industry, which has sparked U.S. surveillance concerns from European countries.

- **Canadian Judges Now Required to Maintain Proficiency with Technology.** On June 9, the Canadian Judicial Council published an updated edition of its *Ethical Principles for Judges* (*Principles*), a set of ethical guidelines for federally appointed judges originally published in 1998. The revision includes the *Principles'* first reference to judges' use of technology and social media. The provision reads, "judges should develop and maintain proficiency with technology relevant to the nature and performance of their judicial duties," with no further explanation as to what constitutes "proficiency." In the U.S., Model Rule 1.1 notes that lawyers must be knowledgeable of "the benefits and risks associated with relevant technology." The *Principles* also state that judges should be cautious when using social media and cognizant of how their social media presence could affect them professionally.

- **President Biden Gives Warning to Putin That Cyberattacks Will Not Be Tolerated.** While meeting with Russian President Vladimir Putin in Geneva, President Biden warned that 16 types of critical infrastructure should be "off limits" to hacks. If the warning leads to concrete plans, these remarks could aid in fighting against cybercrime attacks on the U.S. government and on U.S. companies. *Bloomberg Law* reports that Meg King, director of the science and technology innovation program at Washington think tank Wilson Center, hopes that the conversations at the Geneva summit will lead to meaningful collaboration between Russian and U.S. intelligence officials. King notes that by creating an open channel of information, the U.S. government will be notified of foreign attacks before they take place.

- **The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) Call for Ban on Use of Facial Recognition in Public Spaces.** In a joint opinion, the EDPB and EDPS stated, "A general ban on the use of facial recognition in publicly accessible areas is the necessary starting point if we want to preserve our freedoms and create a human-centric legal framework for AI." The EU regulators expressed concern that certain uses of AI can lead to unfair discrimination. This stance directly opposes drafting EU rules that would allow the technology to be used for public security reasons.

- **Amazon Faces $425 Million EU Privacy Fine.** Luxembourg's data protection commission, the CNPD, has circulated a draft decision sanctioning Amazon's privacy practices. The case concerns whether Amazon's privacy practices on its collection and use of personal data violate Europe's GDPR. If EU privacy regulators

agree, this could be the biggest penalty to date under the bloc's privacy law.

TROUTMAN PEPPER TEAM SPOTLIGHT: ANGELO STIO

Angelo A. Stio III is a partner in our New Jersey and New York offices and serves as a Cybersecurity, Information Governance, and Privacy Group section leader, where he oversees the incident response section. Angelo works with entities across various sectors on incident response and compliance issues involving U.S. federal and state laws governing consumer privacy, the privacy of education records, and patient privacy. He has successfully defended clients in individual and class matters involving privacy and security issues in various jurisdictions throughout the country, earning distinctions from the New Jersey *Super Lawyers* listing in business litigation (2011-2017), and from *Benchmark Litigation* (2019-2021) as a local litigation star.

A frequent writer and lecturer on privacy and security issues, Angelo is accredited by the International Association of Privacy Professionals as a Certified Information Privacy Professional/United States (CIPP/US)[1], and he currently serves as the co-chair of the New Jersey State Bar Association Privacy Law Committee.

In his free time, Angelo is an adjunct professor, where he teaches a course on Cyber Ethics and serves on the State of New Jersey's District VII Attorney Ethics Committee.

WEBINARS

- **COPPA's Next Act: Everyone Is Eager to Protect Children's Privacy | Wednesday, July 28, 2021 | 3 p.m. ET (12 p.m. PT)**

  In this webinar, Troutman Pepper Partner Tim Butler and Associates Chelsea Lamb, Carlin McCrory, and Matthew White will provide real-world guidance on the Children's Online Privacy Protection Act (COPPA or Act), including pro-tips for complying with the Act, trends emerging from government enforcement actions and private litigation matters, and recent legislative and regulatory efforts to strengthen privacy protections for children. To register, please click here.

  Please also watch for our invitation to our upcoming Colorado Privacy Act (CPA) webinar series.

RECENT TROUTMAN PEPPER PUBLICATIONS

- New York City Enacts Biometrics Law for Food and Drink Establishments, Entertainment Venues, and Retail Stores

- Colorado Passes Comprehensive Data Privacy Law

- Biden Signs Executive Order Intended to Improve the Federal Government's Cybersecurity

---

**Rachel Goldner and Camille Sanches are 2021 summer associates with Troutman Pepper and not admitted to practice law.*

[1]The Supreme Court of New Jersey has not approved the CIPP designation under New Jersey Rule of Professional Conduct 7.4.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management