Articles + Publications | April 2022

More Privacy, Please – April 2022

WRITTEN BY

Molly S. DiRago | Rachel Buck Hodges | Ronald Raether, Jr. | David N. Anthony | Angelo A. Stio, III | Ashley L. Taylor, Jr. | Jonathan "Grady" Howe | Robyn W. Lin | Lissette Payne | Kamran Salour

Editor's Note: Utah became the fourth state in the nation to successfully pass a comprehensive privacy bill, following California, Colorado, and Virginia. Meanwhile, seven other states failed at their own attempts, including Florida, Washington, and Indiana. There also has been a flurry of biometric privacy bills largely modeled on Illinois' Biometric Information Privacy Act (BIPA), although none have yet passed. Illinois continues to be a large source of privacy litigation, including a Seventh Circuit affirmation of dismissal due to an arbitration clause in favor of Snap, Inc. On the regulatory side, the Federal Trade Commission (FTC) proposed a consent order against CafePress over allegations the company failed to implement reasonable security measures, while self-regulatory industry watchdog the Children's Advertising Review Unit levied a violation of the Children's Online Privacy Protection Act (COPPA) against kids app TickTalk Tech LLC. In international updates, the European Union (EU) and the U.S. announced a new trans-Atlantic data privacy framework to effectuate cross-border transfers of personal data that would replace the EU-U.S. Privacy Shield. Norway's data protection regulator urged companies to review data transfers in light of Russia's invasion on Ukraine, and the Irish data protection commission fined Meta Platforms 17 million euros over a series of 12 data breaches.

US Laws and Regulation

- **Utah Enacts Privacy Act.** Utah became the fourth state to enact a comprehensive state privacy law, closely resembling both the Virginia Consumer Data Protection Act (VCDPA) and the Colorado Privacy Act (CPA). Unlike the VCDPA and the CPA, however, (1) there is no right to correct data, (2) data controllers are not required to implement an appeals process when a consumer request is denied, (3) there is no data protection risk assessment requirement, and (4) consumer consent is not required prior to processing the sensitive data of adult consumers. This act will go into effect on December 31, 2023. For more analysis, click here.

- **2022 State Privacy Legislative Sessions.** As of March 22, 11 states wrapped up their 2022 legislative sessions. Of these 11 states, seven states considered privacy legislation, namely Florida, Washington, Indiana, Virginia (amendments to enacted regime), West Virginia, Wisconsin, and Utah. Privacy bills passed out of at least one house in Utah, Florida, Indiana, and Wisconsin. While such signs of potential momentum are noteworthy, the final outcome of these early sessions largely mirrored the results of 2021 legislative sessions, with many bills failing to pass. So far, Utah is the only state to pass a comprehensive privacy bill in 2022. For more information on the 2022 state privacy legislative season, please click here.

- **2022 State Biometric Privacy Laws.** In the first quarter of 2022, seven states introduced biometric laws — California, Kentucky, Maine, Maryland, Massachusetts, Missouri, and New York — generally based on Illinois'

Biometric Privacy Act (BIPA). These new biometrics bills potentially create new avenues on which to sue businesses, and also indicate that state legislatures are cracking down on the collection, use, and processing of biometric information. Companies that collect and use biometric information should prepare for compliance in light of potential enactment of these laws. For a comparison of these bills to BIPA, please click here.

US Litigation and Enforcement

- **Continued Wait for CPRA Regulations.** California Privacy Protection Agency Director Ashkan Soltani recently announced that the agency would not meet its July 1 deadline to promulgate regulations. He stated that formal proceedings, including public hearings, will continue into Q3, with rulemaking completing in Q3 or Q4. While Soltani offered no explanation, the announcement is unsurprising given prior comments made at the September 2021 board hearing. For more analysis, click here.

- **Time's Up for Kids' Smartwatch Maker.** The Children's Advertising Review Unit (CARU) — a branch of self-regulatory industry watchdog BBB National Programs — recently examined the data handling and sharing practices of TickTalk Tech LLC (TickTalk). TickTalk owns and operates a smartwatch for kids known as TickTalk 4, as well as a coordinating app for the product. CARU determined the company violates the Children's Online Privacy Protection Act (COPPA) because it fails to provide clear, complete, and non-confusing notice of its children's information collection practices in its privacy policy, and it fails to provide direct notice to parents as required by COPPA. CARU concluded that TickTalk neglects to offer a means for parents to provide verifiable consent prior to collecting information from children. In response, the company agreed to overhaul how it obtains parental permission.

- **Seventh Circuit Sides With Snapchat in BIPA Arbitration Fight.** On March 24, the Seventh Circuit affirmed an Illinois federal court's dismissal of a BIPA case made against Snap, Inc. due to an arbitration provision in the company's terms of service. The lower court sent the case to arbitration when Snapchat alleged that a minor misrepresented her age when joining Snapchat. The minor launched her original suit in state court in November 2020, claiming that Snapchat violated her and other Illinois users' biometric privacy rights by incorporating lenses and filters on its social platform that scan facial features without informed consent. Snap removed the case to federal court before moving to compel arbitration. The district court found that the plaintiff was bound by the arbitration provision despite the plaintiff's defense to the enforceability of Snapchat's terms of service. The plaintiff asserted her age as a minor as a defense to the enforceability of the contract because she was 11 years old when she signed up for Snapchat. The Seventh Circuit held this defense was a question for the arbitrator.

- **FTC Targets CafePress Data Breach.** The FTC proposed a consent order against CafePress over allegations the company failed to implement reasonable security measures to protect sensitive information stored on its network, including Social Security numbers, inadequately encrypted passwords, and answers to password reset questions. According to the FTC's complaint, a hacker exploited the company's security failures in February 2019 to access millions of email addresses and passwords with weak encryption, more than 180,000 unencrypted Social Security numbers, and tens of thousands of partial payment card numbers and expiration dates. Some of this information was found on the dark web. The allegations also stated the company failed to properly investigate the breach for several months despite multiple warnings from individuals and a foreign

government. The proposed settlement will require Residual Pumpkin Entity, LLC — the former owner of CafePress — to pay $500,000 in redress to victims of the data breach.

- **Illinois Court Rejects Macy's Early Appeal on BIPA Claim.** On March 18, the Northern District of Illinois rejected Macy's motion to certify an interlocutory appeal, challenging aspects of the court's denial of Macy's motion to dismiss. Macy's, a co-defendant in the *In re: Clearview AI, Inc. Consumer Privacy Litigation*, asked the court to certify three questions, including "whether, in light of the United States Supreme Court's decision in *TransUnion*, allegations of bare statutory violations of Illinois' [BIPA], unaccompanied by allegations of actual harm, confer Article III standing." The court rejected this question for interlocutory appeal, noting that *TransUnion* — which analogized FCRA claims to common law torts of defamation — did not affect Seventh Circuit precedent analogizing BIPA violations to common law privacy torts sufficient in their own right to show injury-in-fact without further tangible consequences. The court held that the plaintiffs sufficiently alleged their BIPA 15(b) claim based on the harm associated with the invasion of their private information. The court also rejected Macy's certified questions relating to plaintiffs' BIPA 15(c) claim and claims under California and New York statutes and common law.

- **Bed Bath & Beyond Settles With Class Over BIPA Allegations.** Online gift platform Personalizationmall.com, owned by Bed Bath & Beyond, submitted a preliminary settlement of $4.5 million for approval. Workers alleged that Personalizationmall.com violated BIPA by failing to obtain informed consent before requiring them to scan their fingerprints to clock in and out of work. The proposed settlement will pay each settling class member between $569 and $952 before fee and other cost reductions, depending on the final claim response rate. Class members will have 180 days to cash their checks. If approved, the settlement will resolve two class actions, alleging nearly identical claims that were consolidated in 2020. The settlement now awaits Judge Thomas Durkin's approval.

International Regulation and Enforcement

- **US and Europe Announce Agreement on New Trans-Atlantic Data Privacy Framework to Replace EU-US Privacy Shield.** The United States and the European Commission recently announced an "agreement in principle" on a new trans-Atlantic data privacy framework, which seeks to effectuate cross-border transfers of personal data from the European Union (EU) to the U.S. In *Data Protection Commissioner v. Facebook Ireland Ltd, Maximilian Schrems and Intervening Parties* (Schrems II), the Court of Justice of the European Union had invalidated the EU-U.S. Privacy Shield, which, at the time, was one of the primary mechanisms used for the cross-border transfers of personal data from the EU to the U.S. The new agreement provides a level of reprieve for businesses and organizations throughout the U.S. and Europe, seeking clarity and guidance on best practices to manage cross-border data transfers. To learn more about this agreement, click here.

- **Norway Urges Review of Data Transfers to Russia, Ukraine.** In light of Russia's invasion on Ukraine, Norway's data protection regulator is calling on companies that export personal data to Russia and Ukraine to reassess exchanges to ensure they are still legal. Under the GDPR, companies that export data to recipients outside of the European Economic Area (EEA) must have a lawful basis. These countries must have been deemed to have data protections on par to the EEA and must conduct an assessment to ensure that the transferred data will continue to be equally well-protected once it leaves the region.

- **Irish Data Protection Commission Fines Meta.** The Irish Data Protection Commission fined Meta Platforms (formerly known as Facebook) 17 million euros over a series of 12 data breaches from June to December 2018. The inquiry found that Meta Platforms infringed Articles 5(2) and 24(1) of the GDPR by failing to have in place appropriate technical and organizational measures to enable it to readily demonstrate the security measure implemented to protect EU users' data. This decision represents the collective views of both the Irish Data Protection Commission and its counterpart supervisory authorities throughout the EU.

Troutman Pepper Team Spotlight: Kim Phan

Partner Kim Phan practices privacy and data security law in the firm's Consumer Financial Services Practice Group. She also assists companies with data breach prevention and response, including establishing effective security programs before a data breach and assessing breach response obligations following a breach.

Based in Washington, D.C., Kim 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 also provides extensive client e-commerce and mobile counseling, including adapting an augmented reality mobile game for a retail client, conducting online behavioral advertising assessments of websites to update and enhance website privacy policies, adapting website functions for accessibility in compliance with the Americans with Disabilities Act (ADA), and establishing employee training on social media interactions with consumers.

Kim's practice also focuses 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. Kim also has counseled clients through state attorneys general and departments of consumer protection investigations.

Recent Troutman Pepper Publications

- **Déjà Vu? Outcomes of Privacy Legislation in 2022 State Legislative Sessions**
- **Utah Consumer Privacy Act Awaiting Signature**
- **US and Europe Issue Joint Statement Announcing Agreement on New Trans-Atlantic Data Privacy Framework to Replace EU-US Privacy Shield**

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- eDiscovery + Data Management