Articles + Publications | March 2021

More Privacy, Please – March 2021

WRITTEN BY

David N. Anthony | Ronald I. Raether Jr. | Ashley L. Taylor, Jr. | Angelo A. Stio III | Wynter L. Deagle | Rachel Miklaszewski | Sharon R. Klein

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

- **Virginia Enacts Consumer Data Privacy Legislation.** Virginia has become the second state with its own comprehensive data privacy legislation. Following passage by both houses of Virginia's state legislature with large bipartisan majorities, Virginia Governor Ralph Northam signed the Consumer Data Protection Act (CDPA) into law on March 2, 2021. It should come as no surprise that Virginia's CDPA is similar, but not identical to, California's CCPA. Indeed, as we discussed in our 2019 *Bloomberg Law* article, *So the CCPA is Ambiguous – Now What?*, all privacy laws derive from the same core foundational principals, namely the Fair Information Practice Principles. The CDPA includes similar concepts and provisions, such as giving Virginians the right to determine whether their data is being collected and processed, to ask for a copy of their data, to correct inaccuracies, to ask for the deletion of personal data, and to opt out of processing personal data that may be used for targeted advertising, sale, or consumer profiling. The CDPA gives the Virginia attorney general exclusive enforcement authority, and does not provide for a private right of action. The CDPA becomes effective Jan. 1, 2023, the same day most of the provisions of the California Privacy Rights Act, the updated voter-approved version of the California Consumer Privacy Act, will take effect. The CDPA will apply to all businesses that control or process data for at least 100,000 Virginians, or those commercial entities that derive at least 50% of their revenues from the sale and processing of consumer data of at least 25,000 customers.

  Troutman Pepper's forthcoming five-part series on Virginia's CDPA will provide a detailed overview of the Act and how it compares to California's approach to privacy under the CCPA and CPRA, including a discussion of consumer rights, notice and disclosure obligations, data processing obligations, and enforcement. At the conclusion of the series, Troutman Pepper will host a webinar on the CDPA. Stay tuned for registration information.

- **DFS Releases Its Cyber Insurance Risk Framework.** Although DHS Cybersecurity Insurance Working Sessions released reports about the sessions a few years ago, and the National Association of Insurance Commissioners (NAIC) had formed a working group that issued recommendations in 2017, New York's Department of Financial Services is the first U.S. regulator to issue specific guidance for property/casualty insurers writing cyber insurance. As cybercrime becomes more common and more costly, this new cyber

insurance framework seeks to "foster the growth of a robust cyber insurance market" to help protect against the growing number of cyber threats faced by organizations in modern life. Among other things, the DFS recommends against paying ransom payments, which it contends "fuels the vicious cycle of ransomware" and does not guarantee that an organization will get its data back or that criminals will not use that stolen data in the future. For a full copy of the Framework, go to the DFS website.

- **Oklahoma and Utah Lawmakers Introduce Privacy Bills.** The Oklahoma House of Representatives introduced House Bill 1602 to enact the Oklahoma Computer Data Privacy Act (Act). As drafted, the Oklahoma Computer Data Privacy Act applies to certain businesses that collect consumers' personal information and gives consumers the right to request disclosure and deletion of information. Similarly, Utah's state Senate introduced Senate Bill 200 to enact the Utah Consumer Privacy Act. Like Oklahoma's Computer Data Privacy Act, Utah's Consumer Privacy Act gives Utah consumers the right to access, correct, and delete certain personal data, among other things. Oklahoma and Utah now join Alabama, Arizona, Connecticut, Florida, Kentucky, Minnesota, New York, Virginia, and Washington on the list of states considering comprehensive privacy bills.

- **FTC Releases Fraud Report.** On February 4, the FTC announced it received over 2.1 million fraud reports in 2020. The most common type of fraud reported to the FTC related to "imposter scams." The second most common, with an elevated surge during the start of the pandemic, relates to online shopping. Compared to 2019, consumers reported a $1.5 billion loss increase in 2020, totaling nearly $3.3 billion in losses. For those interested in reviewing the full breakdown of reports received last year, click here. To read the February 4 announcement, click here.

- **FTC Acting Chairwoman Details Priorities at Future of Privacy Forum.** Speaking at the February 10 Future of Privacy Forum, FTC Acting Chairwoman Rebecca Kelly Slaughter emphasized the need for strong privacy legislation at the federal level. She also called for FTC staff to be more creative in fashioning settlements, suggesting disgorgement of data as one tool in the FTC "toolbox" when pursuing misconduct. Slaughter discussed the current pandemic and its resulting privacy and security issues, including those related to technology, that have become more prevalent due to the pandemic, such as ed-tech and health apps. Finally, Slaughter addressed racial equity and the FTC's role in fighting racial injustice. For Slaughter's full remarks, click here.

U.S. LITIGATION AND ENFORCEMENT

- **Eleventh Circuit Invites Supreme Court to Address Circuit Split on Article III Standing for Data Incident Plaintiffs.** Highlighting the disagreement among federal appellate courts on the type of harm required to establish Article III standing in the context of a data breach, the Eleventh Circuit affirmed a district court's dismissal of the plaintiff's purported class action complaint, holding that a "substantial risk of identity theft, fraud, and other harm in the future as a result of the data breach" is ***not*** sufficient to establish standing. In so doing, the Eleventh Circuit joins the Second, Third, Fourth, and Eight circuits. In contrast, the Sixth, Seventh, Ninth, and D.C. circuits have found similar allegations sufficient to support Article III standing in comparable scenarios at the pleading stage. The Eleventh Circuit's thorough analysis — occupying eight of the opinion's 26 pages — lays the groundwork for Supreme Court review and is a not-so-subtle invitation for the justices to weigh

in, with the concurring opinion specifically expressing the hope that "the Supreme Court will soon grant certiorari in a case presenting the question of Article III standing in a data breach case." As we previously discussed in December 2020, the Supreme Court granted cert in *Ramirez v. TransUnion LLC* to consider "whether either Article III or Rule 23 permits a damages class action where the vast majority of the class suffered no actual injury, let alone an injury anything like what the class representative suffered." While not a data breach case, *Ramirez* offers an opportunity for clarity in the standing context as it applies to class actions. Troutman Pepper's analysis of the decision and the current landscape of standing in data breach cases can be found here.

- **The Seventh Circuit Lets Clearview BIPA Standing Decision Stand.** On February 16, the Seventh Circuit declined to revisit its prior decision upholding a unanimous District Court for the Northern District of Illinois opinion rendered last month in *Thornley v. Clearview AI, Inc.*, holding that "allegations matter" and that the plaintiffs had carefully crafted their allegations to avoid litigating their suit in federal court by alleging only a general, statutory violation rather than the concrete and particularized harm necessary to support Article III standing in federal court. The case will be remanded to the Circuit Court of Cook County to litigate the plaintiffs' claim that Clearview AI, a technology company that "scrapes" pictures of people on public social media websites and then scans the faces to create a searchable, geotagged database of individuals, violated Illinois's Biometric Information Privacy Act (BIPA) by unlawfully profiting from the plaintiffs' biometric data. However, on February 22, Clearview AI filed a motion to stay the litigation, pending its writ of certiorari to the Supreme Court. Clearview AI contends that the case presents substantial unresolved questions about whether an allegation that there was a transfer or sale of biometric information in violation of BIPA necessarily alleges an injury-in-fact for purposes of Article III standing. *Thornley* denotes one of several cases in the past year that have attempted to elucidate federal standing issues for cases brought under BIPA. Currently, the body of law is far from settled, as Justice Hamilton conceded in his *Thornley* concurrence, where he noted that he was unable to "extract from these different lines of cases a consistently predictable rule or standard." The Supreme Court's forthcoming decision in *Ramirez v. TransUnion LLC* may add clarity on the pleading requirements for Article III standing in BIPA cases.

- **ByteDance Agrees to $92 Million Privacy Settlement.** TikTok's Chinese parent company ByteDance recently agreed to pay $92 million to settle a multidistrict litigation (which rolled up 21 putative class-action lawsuits). The suit alleged that TikTok and ByteDance illegally collected and used a broad array of personal information, including biometric data, to track and profile TikTok users for the purpose of, among other things, profiting from ad targeting. While the core claims asserted violations of the Illinois Biometric Information Privacy Act, the complaint also alleged a number of other statutory, common law, and constitutional claims, including violation of the Computer Fraud and Abuse Act, California Comprehensive Data Access and Fraud Act, Video Privacy Protection Act, and California Constitutional Right to Privacy. The structure of the $92 million settlement will allow each member of the "national" class to claim one share and members of the Illinois subclass to claim six shares. In their motion for preliminary approval of the settlement, the plaintiffs' counsel indicated that they do not expect a high percentage of the class to file claims, instead describing likely payouts for hypothetical claims rates from 1.5% ($383.33 for Illinois, $63.89 for everyone else) to 20% ($28.75 for Illinois, $4.79 for everyone else) of the class. If every qualified member of the class filed for a claim, however, recovery would be a maximum of $5.75 for Illinois users and $0.96 for non-Illinois users. Finally, the settlement does not require TikTok to cease its collection, storage, and use of sensitive data, but rather to update its privacy policies to make sure those activities are more clearly disclosed "and in compliance with all applicable

laws."

- **Yodlee Loses Bid to Dismiss California Privacy Class Action.** On February 16, the District Court for the Northern District of California ruled that financial data aggregator Yodlee, Inc. and its parent company Envestnet, Inc. must continue to face consumers' claims that they secretly collected and sold users' personal financial data. The complaint alleges that Yodlee, which develops software applications for financial institutions, surreptitiously retains a user's bank login information when the software is utilized and then uses that information to extract data from the user's account — which it ultimately aggregates and sells. Finding that the plaintiffs "have an expectation of privacy in their personal financial data," which they allege that Yodlee collected without their consent, the court's order leaves intact claims for invasion of privacy, unjust enrichment, violation of California Civil Code § 1709 (fraudulent deceit), and violation of California's Anti-Phishing Act of 2005. The court dismissed claims brought under the federal Stored Communications Act, the federal Computer Fraud and Abuse Act, and under California's Unfair Competition Law and Comprehensive Data Access and Fraud Act, but gave the plaintiffs leave to amend their complaint. The court also reserved ruling on Envestnet's motion to dismiss, pending limited discovery on the plaintiffs' alter ego theory.

- **At Least Two Law Firms Suffer Data Breach as a Result of Accellion Hack.** Both Goodwin Procter and Jones Day announced that their confidential data was accessed during the sophisticated cyberattack on Accellion's File Transfer Appliance (FTA) product that continued into January 2021. Both Goodwin Proctor and Jones Day have revealed that some client information may have been accessed as a result of the breach. A website linked to a hacker known as Clop has posted documents said to be from Jones Day, including a memo to a judge labeled a "confidential mediation brief," according to *The Wall Street Journal*. Another is a cover letter for "confidential documents." For more information, *com*, *Law360*, *Above the Law*, *The Wall Street Journal*, *Bloomberg Law*, and the *ABA Journal* all have coverage.

INTERNATIONAL REGULATION AND ENFORCEMENT

- **UK ICO Publishes Data Analytics Toolkit.** The U.K. Information Commissioner's Office developed a toolkit for organizations utilizing data analytics on personal data. As part of the ICO's artificial intelligence priority work, the toolkit offers key practices that will help organizations embed data protection from the outset when employing data analytics. The ICO said starting analytics with data protection is "a crucial step to gaining public trust and confidence in the technology and how your organisation is using people's data."

- **Clearview AI's Biometric Database Ruled Illegal in Canada.** On February 3, Clearview AI's biometric database was declared unlawful in Canada. The decision comes just a week after Germany's Hamburg Commissioner for Data Protection and Freedom of Information determined that the database also violates the General Data Protection Regulation (GDPR). Clearview AI has amassed a vast collection of more than three billion facial images by scraping publicly available data and using its algorithmic software to derive "faceprints" from these images, creating a trove of biometric information that is searchable by the company's clients. In announcing the outcome of a yearlong investigation, Canada's Office of the Privacy Commissioner concluded that Clearview AI's practices represented "mass surveillance" and were "illegal."

- **EU Member States Agree on Council's Text for the ePrivacy Regulation.** On February 10, the EU member states agreed on a negotiating mandate for revised rules on the privacy and confidentiality of electronic communications, which allows the Portuguese presidency to start discussions with the European Parliament on the final text of the planned ePrivacy regulation. An update to the existing ePrivacy directive of 2002 to address new technological and market developments (such as cross-contextual behavioral advertising, Voice over IP, and web-based email and messaging services), is long overdue. The current proposal, however, is likely to undergo additional revisions during negotiations with the European Parliament. The regulation will apply two years after its publication in the *EU Official Journal*.

TROUTMAN PEPPER TEAM SPOTLIGHT: CHARLIE PEELER

In January 2021, Troutman Pepper welcomed former U.S. Attorney for the Middle District to Georgia Charlie Peeler to the firm. Charlie represents clients in civil and criminal government enforcement actions, litigation arising from cyberattacks and data breaches, and complex commercial disputes.

Charlie also works proactively with clients to develop ethics and compliance programs and conduct internal investigations. As the former U.S. Attorney for the Middle District of Georgia, Charlie gained invaluable experience leading government investigations into and prosecutions of cybercrimes, including those arising out of ransomware attacks, business email compromises, cyberstalking, and online scams. To best assist clients in preventing and responding to cyberattacks, Charlie leverages his valuable insight and extensive experience gained from working with federal law enforcement, including the DOJ Computer Crime and Intellectual Property Section and the Department of Justice Subcommittee on Cybercrime and Intellectual Property Issues. In his (admittedly limited) free time, Charlie enjoys playing golf, adventuring outdoors, and spending time with his wife and children.

RECENT TROUTMAN PEPPER PUBLICATIONS

- FDCPA Standing: Seventh Circuit District Court Affirms That "Annoyance and Confusion" Without Detrimental Action is Insufficient to Establish an Injury in Fact
- Data Compliance Issues for Cos. Making, Using Vaccine Apps
- DFS Releases Its Cyber Insurance Risk Framework
- Calling SCOTUS: Eleventh Circuit Invites Supreme Court to Address Circuit Split on Article III Standing for Data

Incident Plaintiffs

- District Court Grants Plaintiff's Motion to Certify Class in Part, Refusing to Credit Testimony Regarding Unwritten Consent Policies
- Mastercard to Provide Additional Transaction Detail
- The FDCPA and Foreclosures: Ninth Circuit District Court Denies Defendant's Motion for Summary Judgment on All Counts

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber