A Wave of New Data Privacy Suits Tests Novel Theories

In the absence of a comprehensive federal data privacy law, plaintiff lawyers are testing new theories of liability under state laws—and they are more frequently being met with success. Recent data privacy-related lawsuits against well-known online companies have resulted in large settlements, including Facebook ($650 million), TikTok ($92 million), Zoom ($85 million), and T-Mobile ($350 million). [1] Given the increasing collection and use of personal data by so many businesses—from healthcare services, to digital advertising, to biometrics-based security—this trend is likely to only increase. This article provides an overview of the theories plaintiffs have been most actively pursuing over the last 12 months.

I. Biometric Information Cases

The Illinois Biometric Information Privacy Act ("BIPA") regulates the collection, use, retention, and destruction of individuals' biometric identifying information, such as fingerprints, retina scans, and facial geometry scans.[2] BIPA applies to any private entity that operates or does business in Illinois. Broadly speaking, it requires businesses in possession of biometric information to: (a) develop and disclose written policies around the retention and destruction of biometric information, (b) obtain consent to collect, disclose, or profit from an individual's biometric information, and (c) safeguard biometric information in a manner that is "the same as or more protective than" the way the entity protects its other confidential information. The Statute authorizes a private right of action, allowing individuals to recover $1,000 per negligent violation and $5,000 per intentional or reckless violation. Critically, with the limited exception of claims under Section 15(a), plaintiffs need not establish damages beyond violation of their rights under the Statute to sue under BIPA's other provisions.[3]

On October 12, 2022, a federal jury awarded $228 million in damages under BIPA against BNSF Railway, operator of one of the largest freight railroad networks in North America.[4] The jury found that BNSF had recklessly or intentionally violated BIPA 45,600 times when it collected its employees' fingerprint scans without their consent, over and over when they checked in and out of work.[5] Remarkably, BNSF did not, itself, collect the data. Rather, the data was collected by a third-party vendor, Remprex LLC. Nonetheless, the jury rejected BNSF's defense that it was not responsible for the method and manner of Remprex's collection and should not be subject to vicarious liability.

Notably, this was the first biometric information case to reach a jury. That is not because judges are disposing of them at the pleading or summary judgment stage. Instead, when the cases are headed for trial, especially if certified as class actions, the defendants have settled. That happened in the seminal *Six Flags* case last year.[6] The jury verdict in *BNSF Railway* confirms that juries will impose the statutory damage amount for each violation of the Statute. It will undoubtedly spur even more BIPA cases.

---

[1] *See In re Facebook Biometric Info. Privacy Litig.*, 2020 WL 4818608 (N.D. Cal. Aug. 19, 2020); *In re Tiktok, Inc., Consumer Priv. Litig.*, 2022 WL 2982782 (N.D. Ill. July 28, 2022); *In re: T-Mobile Customer Data Sec. Breach Litig.*, No. 4:21-md-03019 (July 22, 2022); *In re: Zoom Video Commc'ns, Inc. Privacy Litig.*, No. 20-02155 (N.D. Cal. Oct. 21, 2021).
[2] 740 Ill. Comp. Stat. Ann. 14/1 to 14/25.
[3] *See Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.2d 1197, 1203-07 (Ill. 2019).
[4] *Richard Rogers v. BNSF Railway Company*, Case No. 19-C-3083 (N.D. Ill. Oct. 12, 2022).
[5] *Id.*
[6] *See Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.2d 1197, 1203-07 (Ill. 2019).

Recent BIPA cases have resulted in attention-grabbing settlements. In 2020, Facebook (now Meta) settled a class-action lawsuit alleging violations of BIPA for $650 million.[7] The complaint alleged that Facebook's photo-tagging program improperly collected and stored the class members' facial scans without prior notice or consent.[8] Other settlements include a $92 million class-action lawsuit settlement between the social media network TikTok and users of the platform[9], and a $100 million class-action lawsuit settlement between Google and roughly 420,000 Illinois residents from seven class action suits, who accused the tech giant of violating BIPA by collecting and using their facial data through Google Photos.[10]

And the Illinois statute is just the beginning. New York City's Biometric Privacy Act also has a private right of action.[11] California's S.B. 1189 and Maryland's H.B. 259 propose to enact similar biometric privacy laws with private rights of action.[12] And Texas and Washington have enacted biometric laws, although they do not include private rights of action.[13] Even in states currently lacking specific biometric privacy laws, plaintiffs may be able to bring claims relating to such information under more general statutes. For example, last month, a California state judge allowed claims against Clearview AI to proceed on the theory that Clearview's extraction of face templates from publicly available online photos may violate California residents' rights to privacy under Article 1, § 1 of the California Constitution, their right to publicity under the common law, and their rights under California's Unfair Competition Law.[14] This decision potentially has profound implications because it could provide a basis for the wave of BIPA litigation in Illinois to spread to other states under generic privacy laws—a topic we address in a forthcoming article.

II. "Session Replay" Cases

There has been a recent spate of privacy-based class actions involving "session replay" technology. Session replay technology monitors interactions and submissions on a consumer-facing website. They can be used to capture mouse movements and keystrokes, as well as the consumer's device and browser information. Many companies use session replays to monitor customer behavior, improve user experience, and study how visitors are interacting with their websites or apps. Several class action complaints recently filed in California, Florida, and Pennsylvania challenge the legality of session replay software on the grounds that it constitutes impermissible "wiretapping."

In California, plaintiffs have brought their claims under the California Invasion of Privacy Act ("CIPA"), which provides that anyone who "reads, or attempts to read, or to learn the contents" of a communication "without the consent of all parties to the communication" is in violation of California law. In Florida, plaintiffs have filed claims under the Florida Security of Communications Act ("FSCA"), which similarly provides a cause of action against parties that intercept or use private communications without the consent of all parties to the communication. Plaintiffs in Pennsylvania have sued under Pennsylvania's Wiretapping and Electronic Surveillance Control Act ("WESCA"), which imposes liability on a person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication." Although not identical, these statutes allow plaintiffs to

[7] *See In re Facebook Biometric Info. Privacy Litig.*, 2020 WL 4818608 (N.D. Cal. Aug. 19, 2020).
[8] *Id.* at *6.
[9] *In re Tiktok, Inc., Consumer Priv. Litig.*, 2022 WL 2982782 (N.D. Ill. July 28, 2022).
[10] *Rivera v. Google LLC*, Case No. 2019-CH-00990 (Circuit Court of Cook County Sept. 19, 2020).
[11] *See* NYC Admin. Code §§ 22-1201 – 1205.
[12] Biometric Information, S. Bill 1189, 2021-2022 Reg. Sess. (Cal. 2022); Maryland Personal Information Protection Act, H. Bill 0962, 2022 Reg. Sess. (Md. 2022).
[13] *See* Tex. Bus. & Com. Code § 503.001 and Rev. Code Wash. (ARCW) Title 19, Ch. 19.375.
[14] *Rendeors v. Clearview AI, Inc.*, Alameda Sup. Crt. Case No. RG21096898.

bring suit by alleging (among other elements) that they have not consented to the use of session replay software to record their activity on a website.

A recent Ninth Circuit decision, *Javier v. Assurance IQ, LLC*, No. 21-16351 2022 WL 1744107 (9th Cir. May 31, 2022), emboldened plaintiffs to bring session replay class actions under CIPA in California. In *Javier*, the plaintiff brought a claim in the U.S. District Court for the Northern District of California, alleging that a business' use of session replay software violated CIPA. He alleged that when he visited insurance websites to obtain a quote, the defendant companies recorded his activities on those websites. The district court dismissed the plaintiff's complaint for failure to state a claim. But the Ninth Circuit reversed, concluding "that the California Supreme Court would interpret [the California wiretap statute] to require the prior consent of all parties to a communication." The court remanded the case to the district court to consider whether, based on the complaint's allegations, the plaintiff had impliedly consented to the data collection, and to consider the plaintiff's other arguments that were not previously considered at the motion to dismiss stage. Not surprisingly, *Javier* has led to a surge in session replay cases in California.

Most of the session replay software cases brought in Florida federal district courts have been dismissed for failure to state a claim. In *Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318 (S.D. Fla. 2021), the court dismissed the complaint on the basis that the session replay software did not record conversations in the manner contemplated under the FSCA. The court analogized the session replay software to a security camera in a physical retail store, and held that, under the plain language of the Statute, such activity is not regulated by the FSCA. *Goldstein* and similar decisions seemingly spelled the end of session replay cases under the FSCA.

However, another federal court in Florida reached a different result. In *Makkinje v. Extra Space Storage, Inc.*, 8:21-CV-2234-WFJ-SPF, 2022 WL 80437 (M.D. Fla. Jan. 7, 2022), the plaintiff alleged that the "live chat" function on a storage company's website, which the company recorded, violated the FSCA. The court denied the defendant's motion to dismiss, finding that the plaintiff alleged a plausible claim for relief. In so doing, the court found that the case was different from *Goldstein* "because Defendant's use of session replay software during [plaintiff's] visit to its website recorded more than just her non-substantive browsing movements." The court also noted, however, that the question of whether the FSCA applied to a website's recording of its live chats could be resolved at summary judgment. The Eleventh Circuit has not ruled on a session replay case, but the two district court cases are instructive. In Florida, a FSCA suit challenging the use of a live chat function is likely to survive a motion to dismiss, while a suit challenging the use of session replay software merely to record browsing on a website is not.

The Third Circuit's recent decision *in Popa v. Harriet Carter Gifts, Inc.*, 45 F.4th 687 (3d Cir. 2022) has opened the door for plaintiffs to bring session replay software claims under Pennsylvania's WESCA statute. The plaintiff visited an online store on her smartphone and added a product to her cart. Unbeknownst to the plaintiff, the store was using session replay software to track her interactions with the website. The plaintiff alleged that the store (and a third-party marketing company) violated WESCA. The district court granted summary judgment in the defendant's favor. The Third Circuit reversed, ruling that the defendants' use of session replay software constitutes an "interception" under WESCA, even though the interceptors (i.e., the defendants) were a direct party to the communication. This ruling is likely to spur more cases in Pennsylvania under WESCA.

III. "Meta Pixel" Cases

Since February 2022, over 50 class actions have been filed claiming that Meta Platform's Pixel tracking tool sent the plaintiffs' personal video viewing data from a website to Facebook without their consent, violating

the federal Video Privacy Protection Act ("VPPA").[15] Almost half of these cases were filed in September. Targets have included news outlets, streaming services, and sports organizations.[16] Additional cases are being filed every week. And given the widespread use of the Meta Pixel on websites displaying video content, the list of potential defendants is seemingly endless.

Congress enacted VPPA in 1988 to guard consumers' videotape rental records, after a Washington DC newspaper attempted (unsuccessfully) to shame a Supreme Court nominee by publishing a list of his videotape rentals from a local store. It has since been expanded to bar digital video providers from disclosing personally identifiable information tied to the titles of that consumers' viewed videos without their express consent. Under the Statute, the court may award a prevailing plaintiff "actual damages but not less than liquidated damages in an amount of $2,500," as well as attorneys' fees and litigation costs.[17] There is a circuit split on whether users of free mobile apps or website video players can assert claims under the Act. The Eleventh Circuit has held that merely downloading a free app or visiting a website does not mean that the user is a "renter, purchaser, or subscriber."[18] However, in *Yershov v. Gannett Satellite Information Network, Inc.*, the First Circuit held that a plaintiff who downloaded *USA Today*'s free application was a "subscriber" because he gave the defendants the GPS location of his mobile device, his device identifier and the titles of the videos he viewed, in return for access to Gannett's video content.[19] The court considered this an exchange of sufficient value to trigger VPPA.

Although some cases have been dismissed voluntarily—including cases against National Public Radio, Gamestop, and Bloomberg LP—several have moved past the motion to dismiss stage and into discovery. For example, in one of the first "Meta Pixel" cases, the District of Massachusetts recently denied Boston Globe Media Partners LLC's motion to dismiss, holding that the "VPPA claim plausibly states a claim for relief."[20]

***

Data privacy litigation has been on the rise for years, but it has not come close to peaking. The number of companies that maintain and rely on consumer and employee data will only continue to increase. Meanwhile, the plaintiffs' bar is continuing to invoke statutes passed in the pre-Internet era to circumstances that legislatures may not have foreseen or intended. To limit the risk of exposure, businesses must maintain (and routinely update) conspicuous policies that clearly disclose their collection, use, and sharing of data. The notice and retention provisions of these statutes are not difficult to comply with. Most of these suits spring from mere procedural violations and do not allege data breaches or any actual harm. A consultation with lawyers who have litigated the statutes, and who can develop compliance practices is a much more cost-effect way to dealing with the laws than is writing a nine-figure settlement check.

***

If you have any questions about the issues addressed in this memorandum, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to reach out to:

---

[15] https://news.bloomberglaw.com/privacy-and-data-security/meta-pixels-video-tracking-spurs-wave-of-consumer-privacy-suits

[16] *Id.*

[17] *See* 18 U.S.C. § 2710(c)(1)-(2).

[18] 18 U.S.C.A. § 2710(a)(1). *See, e.g. Perry v. CNN*, 854 F.3d 1336, 1341–44 (11th Cir. 2017); *Ellis v. Cartoon Network, Inc.*, 803 F.3d 1251, 1255–58 (11th Cir. 2015).

[19] *Yershov v. Gannett Satellite Information Network, Inc.*, 820 F.3d 482, 489 (1st Cir. 2016).

[20] *Ambrose v. Boston Globe Media Partners LLC*, 2022 U.S. Dist. LEXIS 168403 (D. Mass. Sept. 19, 2022).

Anthony Alden
Email: anthonyalden@quinnemanuel.com
Phone: 213-443-3159

Stephen Broome
Email: stephenbroome@quinnemanuel.com
Phone: 213-443-3285

Viola Trebicka
Email: violatrebicka@quinnemanuel.com
Phone: 213-443-3243

December 8, 2022