Updates
January 23, 2025
Privacy Law Recap 2024: Class Actions and Mass Arbitrations

Claims involving the alleged collection and use of consumer data continued to drive trends in privacy class actions and mass arbitrations in 2024.

Biometrics Litigation

The Illinois Biometric Information Privacy Act (BIPA) continued to be a significant driver of class-action litigation. In 2024, a series of court opinions and legislative updates brought increased clarity regarding the scope and application of the statute.

In June, the U.S. Court of Appeals for the Ninth Circuit issued an influential opinion clarifying that "biometric identifiers" as defined by BIPA must identify—or at a minimum, be capable of identifying—an individual. *See Zellmer v. Meta Platforms, Inc.*, 104 F.4th 1117 (9th Cir. 2024). In *Zellmer*, the panel held that the alleged biometric data at issue—"face signatures," or numerical representations of a face—were not covered by the statute because they could not be used to identify a person. While the plaintiff offered evidence that face signatures could be used to predict age and gender, the panel reasoned that those predictions do not constitute identification as required by BIPA.

Zellmer solidified a trend towards courts adopting a no-identification defense under BIPA, and others have since followed its reasoning. For example, the U.S. District Court for the Northern District of Illinois dismissed a claim on the grounds that "BIPA only covers those 'retina or iris scan[s], fingerprint[s], voiceprint[s], or scan[s] of hand or face geometry' that are *capable of identifying an individual.*" *G.T. v. Samsung Elecs. Am. Inc.*, No. 21 CV 4976, 2024 WL 3520026, at *7 (N.D. Ill. July 24, 2024) (emphasis added). For this reason, the fact that the technology at issue allegedly performed face scans was not dispositive.

In August, Illinois Governor J.B. Pritzker signed the highly anticipated SB 2979, which significantly reduced potential liability for defendants by amending BIPA to provide that a private entity that collects or discloses "the same biometric identifier or biometric information from the same person using the same method of collection" has committed only a single violation of BIPA for which the plaintiff is entitled to, at most, a single recovery. SB 2979 was enacted in response to the Illinois Supreme Court's ruling in *Cothron v. White Castle Systems*, 216 N.E.3d 918 (Ill. 2023), which created potentially massive exposure for defendants by holding that every individual scan or transmission of biometric data made without the proper disclosures amounted to a separate violation of BIPA, while also holding that damages for such violations are discretionary. The recent amendment also clarified that the statute's requirement for written consent may be satisfied via an electronic signature. Whether these amendments will apply retroactively remains to be seen, with courts taking differing views in pending district court cases. But in either event, these amendments, in combination with *Cothron*'s holding that damages are discretionary, should help contain exposure for defendants going forward.

Wiretapping and Online Tracking Technology Litigation

In 2024, there was no shortage of wiretapping claims, with plaintiffs continuing to unveil new and increasingly innovative theories claiming that pixels, chatbots, session replay software, and other technologies commonly used on consumer-facing websites violate the California Invasion of Privacy Act (CIPA).

One development involved an explosion in demand letters and lawsuits claiming that pixels and other tracking technologies operate as "pen registers" and "trap-and-trace devices" (PRTTs). While the caselaw on this novel theory is still developing, a number have made it past Rule 12. *See, e.g.*, *Moody v. C2 Education Systems*, No. 2:24-CV-04249-RGK-SK, 2024 WL 3561367 (C.D. Cal. July 25, 2024); *Shah v. Fandom, Inc.*, No. 24-CV-01062-RFL, 2024 WL 4539577 (N.D. Cal. Oct. 21, 2024); *Mirmalek v. Los Angeles Times Commc'ns LLC*, No. 24-CV-01797-CRB, 2024 WL 5102709 (N.D. Cal. Dec. 12, 2024). Meanwhile, several state courts have sustained demurrers and dismissed complaints based on similar theories. *See, e.g.*, *Casillas v. Transitions Optical, Inc.*, 2024 WL 4873370 (Cal. Super. Sept. 9, 2024) (explaining that "obtaining IP addresses from ordinary user access does not violate the pen register statute"); *Rodriguez v. Fountain9, Inc.*, 2024 WL 3886811, at *4 (Cal. Super. July 9, 2024) (sustaining demurrer where plaintiff failed to allege any concrete injury from the collection of her IP address).

Another development involves claims based on "session replay"—software that allows website operators to track a visitor's interactions and browsing behavior, such as mouse clicks, keystrokes, search terms, and page visits, often for the purpose of analyzing and improving site design. Nationwide, plaintiffs have filed suits claiming that this technology violates state and federal wiretap laws by capturing the contents of their "communications" with the websites. Although some initial rulings were mixed, courts are increasingly viewing these claims with skepticism, particularly where plaintiffs fail to allege interception of personally identifiable or private information. Most recently, the U.S. Court of Appeals for the Eighth Circuit affirmed dismissal for lack of standing, explaining that it failed to see how the defendant's use of session replay technology invaded the plaintiff's privacy, "especially when she voluntarily conveyed the information she says is private . . . and when the allegations don't suggest that she provided information that would identify her." *Jones v. Bloomingdales.com, LLC*, No. 23-3304, 2024 WL 5205528 (8th Cir. Dec. 24, 2024).

While websites were a significant focus of wiretapping cases this year, another emerging trend in this space targets providers of cloud-based call center software. In several cases, plaintiffs have alleged that by offering customer-configurable features, such as call recording, transcription, voice authentication, and analysis, these providers intercept and record phone calls in violation of CIPA. These cases have seen some success at Rule 12. *See, e.g., Turner v. Nuance Commc'ns, Inc.*, 735 F. Supp. 3d 1169, 1174 (N.D. Cal. 2024) (denying motion to dismiss claims against provider of voice authentication service). Notably, several of these cases involve

allegations that the defendants retain recorded conversations and use them to improve their own machine-learning models and technologies and foreshadow another emerging trend in privacy litigation—that is, claims targeting the collection and use of data to train AI.

Video Privacy Protection Act

The Video Privacy Protection Act (VPPA) has remained a focus of class-action litigation for several years now, and last year was no different. The VPPA prohibits video tape service providers from knowingly disclosing a consumer's video viewing or rental history without consent and provides for statutory damages of $2,500 per violation. In these cases, plaintiffs allege that website operators violate the statute by improperly sharing their viewing histories using the Meta Pixel. While initial district court rulings suggested attempts to limit the reach of the VPPA—for example, by narrowly construing the terms "video tape service provider" and "consumer"—the U.S. Court of Appeals for the Second Circuit recently reversed course, adopting an expansive view of the statute in *Salazar v. National Basketball Association*, 118 F.4th 533 (2d Cir. 2024). In *Salazar*, the plaintiff argued that his subscription to a free online newsletter made him a "consumer" under the VPPA, even though it was unrelated to the video content he claimed he viewed on NBA.com. The district court dismissed the case on the grounds that the statute's definition of "consumer" is limited to audiovisual "goods or services," which the online newsletter was not. The Second Circuit reversed, holding that the term "consumer" should be understood to encompass a "renter, purchaser, or subscriber of *any* of the provider's 'goods or services'—audiovisual or not," including the online newsletter. While the court described its ruling as "narrow," it nevertheless stated that Congress "did not intend for the VPPA to gather dust next to our VHS tapes" and "the VPPA's privacy protections remain as robust today as they were in 1988." As one of the few appellate rulings interpreting the VPPA, *Salazar*'s expansive reading may well reopen the floodgates for a wave of new claims.

Mass Arbitration

Many of these trends also unfolded outside the courtroom. Plaintiffs continued to threaten and bring mass arbitrations, a strategy which involves hundreds or thousands of claimants filing separate—but coordinated—demands, imposing the threat of significant arbitration fees as a means to force settlements. This year saw increased judicial scrutiny around mass arbitration, including rulings addressing claimants' burden to establish arbitrability, and rulings on the enforceability of mass-arbitration procedures.

On one hand, developments requiring claimants to establish arbitrability have created at least some barriers to the immediate availability of arbitration fees. For example, the U.S. Court of Appeals for the Seventh Circuit issued a ruling requiring claimants to do more than simply identify "a generic arbitration agreement and then independently list[] the names and addresses of alleged consumers without doing anything to link those consumers to the agreement" to establish arbitrability. *Wallrich v. Samsung Elecs. Am., Inc.*, 106 F.4th 609 (7th Cir. 2024). The American Arbitration Association also updated its mass-arbitration rules to expand the role of process arbitrators to address party disputes on procedural requirements before defendants incur significant fees.

On the other hand, courts have looked with increasing scrutiny at mass-arbitration terms that appear to be unclear or unconscionable. Most recently, in *Heckman v. Live Nation Entertainment, Inc.*, the Ninth Circuit held that an arbitration agreement was unconscionable and unenforceable and expressed particular concern with provisions requiring batching and bellwether cases, limiting discovery and evidence presentation, and giving defendants unilateral control over arbitrator selection and which cases would proceed in a batch. 120 F.4th 670 (9th Cir. 2024).

This post is part of a series recapping privacy law developments in 2024. Please see the following Updates for further information:

- Privacy Law Recap 2024: Data Security
- Privacy Law Recap 2024: State Consumer Privacy Laws
- Privacy Law Recap 2024: Regulatory Enforcement

Authors

Explore more in

Privacy & Security Privacy Class Action Defense Class Action Defense

Related insights

Update

DOJ’s Final Rule on Data Transfers: Impacts Across Industries

Update

CFPB Proposes Rule To Expand Regulation E to Crypto and Gaming Accounts