

The Privacy Playbook: How Sports, Media, Entertainment, and Apparel Companies Became Litigation Targets

Article

05.06.2026

By Megan McCurdy and Alex Gunning

Online privacy litigation continues to surge—and professional sports is one of its most visible battlegrounds. In the past two years, the NBA fought a data-sharing lawsuit, the Chicago Cubs faced biometric privacy claims over facial recognition at Wrigley Field, and FuboTV settled a viewing-data class action for over \$3 million. These are not outliers. Sports franchises, streaming platforms, media companies, and sportswear brands are squarely in the crosshairs as plaintiffs apply older privacy statutes to modern digital practices.

Three statutory frameworks have done the heaviest lifting: the California Invasion of Privacy Act (CIPA), Cal. Penal Code §§ 631, 637.2, 638.51, the federal Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710, and state biometric privacy laws led by the Illinois Biometric Information Privacy Act (BIPA), 740 ILCS 14/1 et seq. These acts have spawned copycat laws in numerous other states. Each carries its own remedial scheme and complications for companies collecting data at scale—and the cases show how quickly a novel legal theory becomes real financial risk.

The VPPA has produced the highest-profile sports privacy cases to date. Enacted in 1988 after a reporter published Supreme Court nominee Robert Bork's video rental history, 18 U.S.C. § 2710 prohibits video tape service providers from disclosing personally-identifiable information without consent, with liquidated damages of \$2,500 per violation. Plaintiffs have seized on its broad definitions to target companies sharing viewing data with third parties, and *Salazar v. National Basketball Association*, 118 F.4th 533 (2d Cir. 2024) has become a potential bellwether. In *Salazar*, the Second Circuit reversed a lower court dismissal, holding the plaintiff plausibly alleged he was a "consumer" under VPPA by exchanging personal information for NBA newsletter access that was then allegedly shared with third parties. *Id.* at 536. Critically, the Salazar court noted "[t]he

The Privacy Playbook: How Sports, Media, Entertainment, and Apparel Companies Became Litigation Targets

VPPA is no dinosaur statute," and Congress did not intend the law "to gather dust next to our VHS tapes." *Id.* at 553. The Supreme Court denied certiorari in December 2025. However, in another class action filed by the same exact plaintiff, the Sixth Circuit reached the opposite decision, narrowly interpreting VPPA and holding that the same plaintiff could not plausibly raise a claim. *Salazar v. Paramount Global, et al.*, 133 F.4th 642, 651 (6th Cir. 2025). The U.S. Supreme Court accepted certiorari in the Sixth Circuit matter in January 2026, and the case is set for oral argument later this year. *Salazar v. Paramount Global, et al.*, 2026 WL 189831 (Mem) (U.S. Jan. 26, 2026) (accepting cert). In the humble opinion of these authors, SCOTUS's grant of certiorari suggests it is preparing to bring VPPA firmly into the digital era, likely rejecting the Sixth Circuit's narrow view.

The NBA is not alone. In *Burdette v. FuboTV Inc.*, Case No. 23C10351, 2024 WL 2831466 (N.D. Ill. June 4, 2024), Fubo reportedly settled a VPPA class action for over \$3 million after the court denied Fubo's motion to dismiss. In *Coppedge, et al. v. The Athletic, et al.*, Case No. 1:24CV12312 (D. Mass. June 9, 2025), the New York Times-owned sports media platform faces VPPA and New York Video Consumer Protection Act (N.Y. Gen. Bus. Law §§ 670-675) claims for allegedly sharing viewing histories without authorization. That action is now pending in arbitration.

CIPA has carved out its own fast-growing line of attack. Originally enacted to address Cold War-era surveillance, some courts have expanded it to digital privacy disputes. Plaintiffs argue that website tracking constitutes unauthorized interceptions under California Penal Code sections 631, 637.2, and 638.51, with exposure of \$5,000 per violation. In *Camplisson v. Adidas America Inc.*, Case No. 25-cv-603-GPC-KSC (S.D. Cal. Nov. 18, 2025), plaintiffs allege Adidas installed TikTok Pixel and Microsoft Bing tracking on its website, collecting IP addresses and device details without meaningful consent. In denying Adidas' motion to dismiss, the court found these pixels could plausibly constitute pen registers and that the data collection could amount to concrete injury. The case remains active.

On the biometric front, Illinois' BIPA, 740 ILCS 14/15 requires informed written consent before collecting biometric identifiers such as face geometry scans, with damages of \$1,000 per negligent violation and \$5,000 per intentional one. Stadiums, where thousands pass through entry points daily, are particularly high-risk environments. In *Berta, et al. v. Chicago Cubs Baseball Club LLC, et al.*, 25-CV-11138 (N.D. Ill. Sep. 15, 2025), plaintiffs alleged the Cubs used facial recognition at Wrigley Field without BIPA-compliant consent; the case resolved when plaintiffs withdrew their complaints. However, *Dowling v. Sterling Mets L.P.*, 1:24-CV-07092 (E. D.N.Y. Oct. 8, 2024) raises analogous claims under New York law and remains ongoing.

The major sports gaming companies have largely avoided CIPA, VPPA, and BIPA exposure, with their litigation centering on data breaches and deceptive practices. Whether that holds as the gaming industry's digital footprint grows remains to be seen.

The Privacy Playbook: How Sports, Media, Entertainment, and Apparel Companies Became Litigation Targets

The through line is clear: pervasive data collection, aggressive plaintiffs' strategies, and judicial willingness to apply older statutes to new technologies have created a litigation environment every sports, media, apparel, and entertainment company must take seriously. With states increasingly enforcing comprehensive privacy laws, the compliance burden will only intensify—and the stakes, measured in statutory damages that compound by the user, are enormous.

WHAT SHOULD YOUR GAME PLAN BE?

If you're operating in sports, media, or entertainment, a few practical steps go a long way:

- **Audit your tracking stack**

Know exactly what your site and apps are collecting—and where it's going.

- **Revisit your consent flows**

"Buried in the footer" is not going to cut it anymore.

- **Scrutinize third-party tools**

Pixels, analytics, ad tech—these are often where exposure starts.

- **Stay ahead of state law developments**

The regulatory map is expanding quickly and inconsistently.

- **Loop in counsel early**

Especially if you receive a demand letter—these cases tend to follow predictable playbooks.

Alex J. Gunning

Megan McCurdy

RELATED CAPABILITIES

Esports, Sports Technology & Wagering

Sports & Recreation

STINSON

STINSON LLP \ STINSON.COM