Proskauer

The Next Frontier in Sports: Legal Ramifications of Biometric Data and Virtual Reality Innovation

Minding Your Business on **September 30, 2025**

The rapid expansion of biometric technologies in sports has created both significant opportunities and complex legal challenges. The proliferation of wearable devices and data collection tools has ushered in what amounts to a “gold rush” for athletes, teams, universities, and companies seeking to use or commercialize biometric data. Heart rate variability, fatigue indicators, movement efficiency, and other performance metrics are increasingly captured in real time and treated as valuable commercial assets.

Wearable technology first entered the professional sports spotlight when two NBA players were found wearing WHOOP biometric monitors during games without league authorization. Since then, the four major U.S. sports leagues have reached agreements with their players regarding wearable technology. At the college level, the University of Michigan became the first major program to consent to biometric collection through its apparel contract with Jumpman, a Nike division, which authorized use of heart-rate monitors, GPS trackers, and other devices.

More recently, media outlets have sought to broadcast biometric data directly to audiences. At the 2021 Ryder Cup, television coverage highlighted golfers’ heart rates in real time as they teed off before massive crowds. Given that media entities have partnerships with gaming and gambling operators, many see this as a precursor to monetizing biometric data through sports betting. These developments promise gains in performance analysis, fan engagement, and commercial revenue. Yet they also raise pressing legal questions regarding ownership, consent, and privacy.

Privacy and Consent Considerations

Biometric data is unlike other categories of personal information because it is inseparable from the individual. Once compromised, it cannot simply be replaced. Legislatures have recognized this heightened sensitivity and enacted laws that impose strict consent and disclosure requirements.

At the state level, the Illinois Biometric Information Privacy Act (BIPA) and the California Invasion of Privacy Act (CIPA) have been most influential. BIPA requires informed written consent prior to the collection of biometric information, mandates retention schedules, and provides a private right of action with statutory damages. CIPA, while historically focused on communications privacy, has been interpreted to extend to sensitive data and exposes violators to statutory penalties. Litigation under both statutes has been extensive, and sports organizations that collect player data face potential exposure if they do not obtain clear consent and implement safeguards.

At the federal level, there is no comprehensive biometric privacy statute. However, the Federal Trade Commission has warned that misuse of biometric or health-related data may constitute an unfair or deceptive practice under Section 5 of the FTC Act. If biometric data is connected to medical services, the Health Insurance Portability and Accountability Act (HIPAA) may apply, although wearable device companies are generally not covered entities. Many leagues have addressed HIPAA concerns by including provisions in player agreements to reduce risk.

The larger gap is the lack of consistent application of state biometric privacy laws to wearable sports data. The legal definition of "biometric identifier" under BIPA, for instance, is narrow and limited to fingerprints, facial geometry, retina scans, and similar identifiers. Sports biometrics—heart rate, oxygen levels, movement efficiency—do not fall neatly within this definition. This has led some to argue that current regulations do not reach wearable sports technology.

The stakes are significant. If biometric sports data becomes a target for hackers, the consequences could be irreversible. Professional athletes represent high-value targets whose compromised biometric profiles cannot be reset or reissued. Statutory damages under BIPA alone range from $1,000 per negligent violation to $5,000 for intentional or reckless violations, plus attorneys' fees. The risk of significant financial exposure for participants cannot be overstated.

Data Ownership and Contractual Issues

Even apart from statutory privacy obligations, unresolved questions of ownership complicate the legal landscape. Athletes may argue that biometric data generated from their own bodies should belong to them, while leagues and teams may contend that data collected through employment or competition is the property of the organization. These disputes are likely to become more prominent as biometric data is commercialized through sponsorships, media broadcasts, and sports betting integrations.

Innovation and Immersive Training: SlingShot VR

Despite these uncertainties, innovation in biometric space has continued to explode. One emerging example is SlingShot VR, co-founded by former NBA player Alando Tucker and entrepreneur Cody Ross. SlingShot VR is revolutionizing training practices by developing interactive, real-time virtual reality software designed to transform how athletes and police prepare, train and perform. Its patent-pending 3D streaming and motion-tracking technology enables live, full-body motion data to be integrated into immersive training environments.

For athletes, this technology allows training within virtual scenarios where biometric data is not only observed but actively incorporated into performance feedback. This represents a significant leap forward from traditional training methods, merging physiological insight with immersive, data-driven simulation. Companies such as SlingShot VR demonstrate how biometric data and virtual reality can converge to create more effective and individualized training systems. At the same time, it illustrates the importance of embedding legal compliance and privacy protections into the design and deployment of these tools.

Conclusion

The sports biometrics boom represents a transformative moment for the industry. The collection and commercialization of biometric data offer unprecedented opportunities to enhance performance, deepen fan engagement, and expand revenue streams. At the same time, these advances carry legal risks under state and federal privacy laws, as well as unresolved contractual questions regarding ownership and use.

As this market matures, success will require not only technological advancement but also careful navigation of privacy regulations and contractual obligations. The future of sports biometrics will depend on achieving a balance between innovation and the legal safeguards necessary to protect athletes, organizations and consumers alike.

View original.

Related Professionals

- **Courtland Cuevas**
  Associate