Athletes and their Biometric Data – Who Owns It and How It Can Be Used

Article By:
Brian H. Lam

More than ever before, biometric data, a term often used broadly to refer to metrics related to human characteristics, is being collected at a faster pace. Devices of all kinds are now able to track and store data such as fingerprints, heartrate, and other potentially sensitive data. This tracking can be accomplished through a variety of mechanisms including smartphones, watches, and fitness tracking bands of all kinds. Because of the nature of information which can be collected, it is of particular interest in sports.

While the general consumer issues of such data collection are certainly daunting, tracking of biometric data for athletes can present special issues. At the college level, student-athletes may have concerns that the data being collected could be used to make player management decisions that could affect playing time, positions or even scholarship opportunities. At the professional level, athletes may share similar concerns and are worried that the collected data could be used against them come contract negotiation time.

Understanding the Three Part Relationship Is Essential

In most situations where athlete biometric data is being collected there will be three main participants in the data collection scenario: (1) the athlete whose data is being collected; (2) an institution or entity which wishes to use the data, typically a school or professional organization; and (3) the vendor that provides the biometric equipment and incident services. Understanding which entities have what rights and responsibilities regarding biometric data collected will require recognizing where each entity fits in the three part relationship, as well as whether any special circumstances exist that would influence these rights and responsibilities.

In the United States, biometric data collection falls under a patchwork of regulations, at both the federal and state level. The applicable rules are based primarily on the characteristics of the athlete data subject and the institution or entity that wishes to collect the biometric data, the relevant jurisdictions, the specific types of biometric data being collected, as well as any contractual commitments between the parties. Further, there may be contractual rights at play, particularly at the professional level.

Relevant Characteristics Which Determine Applicable Laws
I. Specific Considerations For Student Data Subjects

In most situations the analysis begins with the athlete data subject to collection. Is the athlete a student? If so, consider whether the athlete is a K-12 student which would likely be most relevant in the context of high school athletics. As noted in our firm’s privacy blog, Cal. Ed. Code § 49073.1, requires that local education agencies (county offices of education, school districts, and charter schools) that contract with third parties for systems or services that manage, access, or use pupil records, to include specific provisions regarding the use, ownership and control of pupil records, which could include biometric data.

Further on the private side, the Student Online Personal Information Privacy Act (SOPIPA), requires education technology to comply with baseline privacy and security protections. Former California Attorney General Kamala Harris provided guidance for those providing education technology for K-12 students, which would likely implicate sensitive biometric tied to individual students. Delaware has enacted a similar law. Individuals operating in this space would be wise to check any applicable whether there are any applicable state laws in their situation.

At the federal level, the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) could also be implicated. As a reminder, FERPA applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Under FERPA generally, schools must have written permission from the parent or eligible student in order to release any information from a student’s education record. It also grants parents certain rights which transfer to the student once the student turns 18. The definition of “personally identifiable information” in § 99.3 includes “biometric record” as part of the list that constitute personally identifiable information.

II. Specific Considerations For Biometric Collection Vendors

Vendors that collect biometric athlete data, as well as the business that contract with these vendors should be aware of the Illinois Biometric Information Privacy Act (“BIPA”), on which additional background can be found here. The Act is being actively litigated, and applies to “any ‘private entity’ — including employers — collecting, storing, or using the biometric information of any individual in Illinois — no matter how it is collected, stored or used, or for what reason.” Certainly, professional sports entities as well as the companies they work with in this space should consider their obligations under BIPA.

III. Professional Sports Organizations, Players Associations and Contractual Issues

Certain professional sports leagues and associated player organizations may have their own rules regarding collection and use of biometric data. For example, the National Football League Players Association (NFLPA) via its newly formed athlete-driven accelerator, the OneTeam Collective, has a partnership that makes WHOOP the Officially Licensed Recovery Wearable of the NFLPA.

As part of the agreement between OneTeam Collective and WHOOP:

- NFL players will own and control their individual data collected with the WHOOP Strap 2.0.
- NFL players will design custom licensed bands for the WHOOP Strap for personal use and commercial sale.
- The NFLPA and WHOOP will study the effects of travel, sleep, scheduling, injuries, etc. on
recovery and generate reports to advance player safety and maximize athletic performance.

- NFL players will have the ability to commercialize their WHOOP data through the NFLPA’s group licensing program.

The National Basketball Association’s collective bargaining agreement (CBA) limits how teams may use data collected from wearables. Under the restriction, “data may not be considered, used, discussed or referenced for any other purpose such as in negotiations regarding a future Player Contract or other Player Contract transaction (e.g., a trade or waiver) involving the player," which allows for an arbitrator to impose a fine of up to $250,000 to any team that violates the provision.

The collection of biometric data on athletes is likely to an active area of regulatory interest for years to come.

©1994-2024 Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. All Rights Reserved.

National Law Review, Volumess VII, Number 353