Journal of Technology Law & Policy

Volume XXI – 2020-2021

ISSN 2164-800X (online)

DOI 10.5195/tlp.2021.245

http://tlp.law.pitt.edu

Biometric Monitoring Devices: Modern Solutions to Protecting Athletes' Data Privacy

Tristan A. Dietrick

Abstract

Smartwatches like Fitbits provide users with easy access to quantifiable health data. In the sports industry, tracking this biometric information may be particularly beneficial to athletes, whose livelihoods revolve around their health and fitness. Nonetheless, under the current regime, professional and collegiate athletes' biometric health data are inadequately protected. Data privacy law is still in its infancy, but in the meantime, athletes must consider that motivations to sell or misuse players' biometric information may outpace legal developments.

This Paper will analyze the promise and risk of collecting professional and collegiate athletes' health and biometric data, particularly through fitness wearables. It will provide a closer look at wearables in professional sports and consider the increased risk posed to college athletes. Finally, this Paper will consider possible solutions to maximize the benefits of newfound technology while simultaneously minimizing risks to players' health information, privacy, and personal data ownership.

Biometric Monitoring Devices: Modern Solutions to Protecting Athletes' Data Privacy

Tristan A. Dietrick*

I. INTRODUCTION

Technological developments in health and medicine are altering the way physicians and patients alike approach healthcare.[1] While these developments are promising, they also pose numerous threats in terms of health data privacy and security.[2] Health data is particularly vulnerable and sensitive—relative to other confidential data—due to its sophistication, permanence, and informativeness.[3] Technological developments should be scrutinized such that individual privacy is sufficiently maintained and protected.

Fitness wearables are a simultaneously promising yet concerning development. Smartwatches, such as the Fitbit or Apple Watch, are well-known examples of fitness wearables. In fact, about one in three Americans report at some point having worn a fitness tracker.[4] But Smartwatches are only part of the industry. Armbands, body gear, helmets, brain and eye trackers, and even rings[5] are other examples of fitness wearables that are revolutionizing the collection of health data.

Wearables can intensively monitor health performance through quantifiable data, including measurements of brain and heart function, calorie intake, blood oxygen, sugar levels, ergonomic issues, distance and routes traveled, fatigue, and

* Tristan A. Dietrick is a J.D. Candidate for the Class of 2021 at the University of Pittsburgh School of Law.

[1] Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. MO. B. 76, 76 (2016).

[2] *Id.*

[3] *Id.*

[4] Justin McCarthy, *One in Five U.S. Adults Use Health Apps, Wearable Trackers*, GALLUP (Dec. 11, 2019), https://news.gallup.com/poll/269096/one-five-adults-health-apps-wearable-trackers.aspx.

[5] The Motiv Ring User's Manual, https://www.mymotiv.com/static/assets/the-motiv-ring-users-manual.pdf?intempt_visitor_id=b25157da04a2b1f4126a016c4706e130 (last visited Mar. 7, 2021).

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.245 ● http://tlp.law.pitt.edu

more.[6] Undeniably, easy access to such data gives users an opportunity to take a more active role in maintaining their health.[7] Similarly, employers can use the data to minimize workplace accidents by analyzing risk factors and implementing safer practices.[8] While these wearables become more popular—some scholars predict that they will one day be as ubiquitous as cell phones[9]—it is also important to recognize that, in many respects, wearables provide a window into the lives of their users.[10] If such data is improperly accessed, analyzed, or distributed, it could be detrimental to users, who may be vulnerable to employment or healthcare discrimination, commercial exploitation, and even identity theft.[11]

In the sports industry, wearable fitness trackers collecting and tracking biometric data are quickly generating attention.[12] Biometrics is the "measurement and analysis of any particular physical characteristic, and more specifically refers to methods for doing so." Biometric data are "measurements or records that can be used to identify people as individuals; identifiers may be physiological (such as heart rate, temperature, and blood sample analysis) or behavioral."[13] This Paper will analyze the benefits and risks of collecting professional and collegiate athletes' health and biometric data, particularly through fitness wearables. Part II provides a closer look at wearables in professional sports, while Part III analyzes the increased risk posed to college athletes. Finally, Part IV considers possible solutions to maximize the benefits of newfound technology while simultaneously minimizing risks to players' health information, privacy, and personal data ownership.

---

[6] Kellogg, *supra* note 1, at 76; *see also Wearables at Work: Balancing Function with Privacy, Other Concerns*, 27 No. 5 N.Y. EMP. L. LETTER 6 (May 2020) [hereinafter *Wearables at Work*].

[7] Kellogg, *supra* note 1, at 76.

[8] *Wearables at Work*, *supra* note 6.

[9] Kellogg, *supra* note 1, at 77.

[10] *Id.* at 76.

[11] *Id.*

[12] Cameron Miller, *Surveying Biometric Data Privacy, Ownership, and Usage in American Sports*, U. DENVER SPORTS & ENT. L.J. (2018), https://duselj.wordpress.com/2018/04/11/surveying-biometric-data-privacy-ownership-and-usage-in-american-sports/.

[13] Barbara Osborne & Jennie L. Cunningham, *Legal and Ethical Implications of Athletes' Biometric Data Collection in Professional Sports*, 28 MARQ. SPORTS L. REV. 37, 38 (2017).

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.245 ● http://tlp.law.pitt.edu

II. WEARABLES IN PROFESSIONAL SPORTS

A. Most Professional Sports Leagues Have Passively Considered Wearables in Collective Bargaining Agreements, but They Inadequately Protect Data Privacy

Collective bargaining agreements (hereinafter "CBAs" or "Agreements") of Major League Baseball (MLB),[14] the National Basketball Association (NBA),[15] and the National Football League (NFL)[16] all address biometric data trackers in some capacity. The National Hockey League (NHL) CBA[17]—which expires in 2026 following a four-year extension agreed upon and accepted by the NHL and NHLPA—does not presently mention biometric data tracking. Even so, there are evident discrepancies between the NHL and the Players Association concerning data ownership and future implementation.[18] When the Agreement expires in 2026, wearables are certain to arise in negotiations.[19]

The MLB and NBA Agreements contain specific sections devoted to wearables.[20] Both Agreements generally stipulate that biometric data cannot be used to players' detriments in terms of contract negotiations or commercial use.[21] Further, both leagues maintain that player's use of biometric trackers is voluntary and that their personal data must be made available to the players. Note, however, that while data must be *available* to players, the Agreements do not specifically address who *owns* the data. Both league Agreements fail to ensure that biometric data is confidential and private. However, such terms will hopefully be more explicit in future contracts as the technology develops and ownership issues are resolved through either legislation or litigation.

---

[14] Major League Baseball Collective Bargaining Agreement (2017–2021) [hereinafter MLB CBA].

[15] National Basketball Association Collective Bargaining Agreement (2017–2024) [hereinafter NBA CBA].

[16] National Football League Collective Bargaining Agreement (2011–2019) [hereinafter NFL CBA].

[17] National Hockey League Collective Bargaining Agreement (2013–2026) [hereinafter NHL CBA].

[18] Greg Wyshynski, *Player Tracking Coming to the NHL? It's Complicated*, ESPN (Feb. 28, 2018), https://www.espn.com/nhl/story/_/id/22604597/nhl-great-player-tracking-debate-ethical-questions-fan-access.

[19] Miller, *supra* note 12.

[20] *See* MLB CBA, Attachment 56; NBA CBA, art. XXII § 13.

[21] *Id.*

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.245 ● http://tlp.law.pitt.edu

Unlike the MLB and NBA, the NFL is more conspicuous regarding the permissibility of health data tracking. The NFL Agreement states that the league "may require . . . players to wear during games and practices equipment that contains sensors or other nonobtrusive tracking devices for purposes of collecting information . . . including players' performances and movements, as well as medical and other player safety-related data."[22] Significantly, the Agreement does not identify the party or parties to which the data belongs, nor is there an assurance that data will be made available to players. Further, unlike the MLB and NBA Agreements, the NFL Agreement lacks crucial language in player voluntariness and the prohibition of exploiting player data for contract negotiations or commercial use.

These lack of restrictions should be especially troubling for players.[23] Under the NFL Agreement, for example, the league could seemingly compel players to wear fitness trackers, store and analyze data as it pleases, and subsequently use the data to players' detriments. Moving forward, the NFLPA would be wise to consider restrictions in the MLB and NBA Agreements as health data collection booms and privacy law develops. Other players associations, likewise, should strongly consider privacy and fairness with respect to the collection and ownership of such sensitive data.[24]

B. Under the Current Legal Framework, It Is Unclear Who Has Ownership Rights over Biometric Data

Professional athletes are considered employees of the leagues in which they play rather than independent contractors.[25] While this entitles players to certain protections, such as rights concerning "wages, benefits, player contract negotiations, medical records, insurance, injury grievances, and retirement," leagues and teams still generally own intellectual property generated by players.[26] It is unclear, under employment and privacy law, whether biometric data is owned by players or leagues.

In *Baltimore Orioles v. Major League Baseball Players Association*, the Players Association brought action alleging that "telecasts were being made without the Players' consent and that they misappropriated the Players' property rights in

[22] NFL CBA, art. 51 § 13(c).

[23] Miller, *supra* note 12.

[24] Pablo S. Torre & Tom Haberstroh, *Players Union Looks at Data Protection*, ESPN (Oct. 6, 2014), https://www.espn.com/nba/story/_/id/11652885/nba-players-union-wants-ensure-privacy-data-collection.

[25] Skyler R. Berman, *Bargaining Over Biometrics: How Player Unions Should Protect Athletes in the Age of Wearable Technology*, 85 BROOKLYN L. REV. 543, 553 (2020).

[26] *Id.* at 553–54.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.245 ● http://tlp.law.pitt.edu

their performances."[27] The Association further contended that game broadcasts "without [players'] consent violated their rights of publicity."[28] The Seventh Circuit disagreed, finding that the telecasts were "works made for hire" and fell within the scope of the players' employment.[29] Thus, under current case law, leagues could plausibly own players' biometric data to the extent that it is "work made for hire" and (1) is copyrightable; (2) was prepared by the player; (3) was prepared within the scope of the players' employment; and (4) the parties have not expressly agreed otherwise.[30]

Of course, there are several distinctions between the telecasts at issue in *Orioles* and biometric data.[31] Biometric data is currently not available for broadcasters, although it may not be far out of reach.[32] It is unclear whether the collection/production of biometric data is within the scope of players' employment, particularly where it is not thoroughly analyzed or considered in league CBAs.[33] Moving forward, players associations would be wise to consider how this data may be copyrightable or, more importantly, valuable both in terms of profit and privacy.

As to copyrightability, the Seventh Circuit in *Orioles* held that "the great commercial value of the players' performances indicates that the works embody a modicum of creativity."[34] However, the Court's conclusion is vulnerable because, despite the commercial value of player performances, "copyright law does not and is not intended to extend to every commercially valuable activity."[35] Rather, copyright law is intended "to increase the wealth of arts and sciences . . . not to protect the commercial value of an athlete's performance."[36] Even under *Orioles* broad acceptance that game telecasts' constitute "works made for hire," athelets' claims for copyrighting their data are tenuous at best.

---

[27] Balt. Orioles v. Major League Baseball Players Ass'n, 805 F.2d 663, 665 (7th Cir. 1986).

[28] *Id.* at 671.

[29] *Id.* at 670.

[30] *Id.* at 667.

[31] Berman, *supra* note 25, at 554–55.

[32] *Id.* at 554.

[33] *Id.* at 555.

[34] Balt. Orioles v. Major League Baseball Players Ass'n, 805 F.2d. 663, 665 (7th Cir. 1986).

[35] Paul M. Enright, Comment, *"Sportstrax: They Love This Game!" A Comment on the* NBA v. Motorola, 7 SETON HALL J. SPORT L. 449, 460 (1997).

[36] *Id.*

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.245 ● http://tlp.law.pitt.edu

More recent decisions further scrutinize and narrow the Court's findings in *Orioles*. Although the Seventh Circuit determined that game broadcasts were works made for hire that fell within the scope of players' employment, *National Basketball Association v. Motorola, Inc.* narrowed this rule.[37] In that case, the NBA sued Motorola for producing hand-held pagers that disseminated real-time game information.[38] The NBA alleged that the dissemination amounted to a copyright violation and misappropriation.[39] The Second Circuit differentiated this case from *Orioles* by holding that "game broadcasts are copyrightable while the underlying games are not."[40] That is, in determining that "cameramen and director[s] contribute creative labor to the telecast," the Seventh Circuit opened the door to the possibility that "[p]layers' performances were not sufficiently creative."[41] Moreover, the court in *Motorola* pointed out another major shortcoming of the *Orioles* court's decision: "the lack of caselaw [supporting the *Orioles* decision] is attributable to a general understanding that athletic events were, and are, uncopyrightable."[42] Thus, if players seek to make a claim for their information on copyright principles, they will likely have to do so outside of *Orioles* and the athletic events themselves.

Under traditional copyright principles—which, with respect to data, generally "require a modicum of originality or creativity in the selection or arrangement of data in a compilation, or other indicia of creative authorship"[43]—the *Motorola* rule makes sense. After all, "[g]ranting copyright protection to sporting events would not forward" the goal of copyright law—to promote the progress of science and useful arts.[44] But players should consider that their biometric data may be more than just "hot-news," or time-sensitive information that is valuable to leagues during game time. Although it could be used for hot-news purposes to engage fans, it is still sensitive health data.

While, under *Orioles* and *Motorola*, player data may not be copyrightable, it can still be valuable in other capacities. For example, to the extent that leagues or third parties are collecting, organizing, and utilizing player data, it would not only

---

[37] Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841 (2d Cir. 1997).

[38] *Id.* at 844.

[39] *Id.* at 843.

[40] *Id.* at 848.

[41] Balt. Orioles v. Major League Baseball Players Ass'n, 805 F.2d 663, 669 (7th Cir. 1986).

[42] *Motorola*, 105 F.3d at 847.

[43] Michael J. Bastian, *Protection of "Noncreative" Databases: Harmonization of United States, Foreign and International Law*, 22 B.C. INT'L & COMP. L. REV. 425, 425 (1999).

[44] Enright, *supra* note 35, at 460.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.245 ● http://tlp.law.pitt.edu

be original, but incredibly marketable. To the extent that players are interested in capitalizing on their unique biometric information, they should be permitted to do so. Databases are "the building blocks of knowledge" in the American economy, and players should not be left behind because of inadequately considered CBAs.[45] Uncopyrightable (i.e. noncreative) databases—including those of collected players' information—may be protectable under other doctrines of law, including misappropriation.[46] After all, an interest is not "disqualified from protection simply because it is not ownable in the usual sense."[47]

Regardless, players should recognize the data's value and ensure that they acquire ownership, possessory rights, or some form of consideration in return for league use. Rather than wait for the issues to arise in litigation, players associations should negotiate clearer terms in CBAs directly addressing that players own their biometric data.

C. Data Collection and Ownership Poses Problematic Conflicts of Interest Concerning Player Data and Sports Management

It is unclear whether leagues have ulterior motives regarding data tracking. In fairness to both the leagues and players unions, CBAs are not negotiated every year and usually have terms greater than five years.[48] Thus, they are not particularly adept at accounting for new technological and societal developments, especially when they arise so quickly.[49] Considering the limited space devoted to wearables in the "Big Four" sports leagues' CBAs, it is possible that data tracking practices were not extensively contemplated.

Regardless, there are countless conflicts of interest pertaining to players' biometric data and sports management.[50] Although contract negotiations and selling sensitive data are briefly addressed in the MLB's and NBA's CBAs, there are other elements of biometric data ownership that could be problematic for teams, including

[45] Bastian, *supra* note 43, at 426.

[46] *Id.* at 428.

[47] *Id.* at 427.

[48] Berman, *supra* note 25, at 545.

[49] *Id.*

[50] Torre & Haberstroh, *supra* note 24.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.245 ● http://tlp.law.pitt.edu

improper incentives to misuse or undermine players' data.[51] The commercialization of data is also insufficiently addressed in league Agreements.[52]

At the very least, some scholars suggest that professional sports leagues and teams—which are highly focused on profitability and immediate return on investment—are inadequately motivated to consider long-term implications of biometric data.[53] The dangers of the Big Four's preoccupation with short-term profitability is well-documented, such as when the NFL attempted to cover up data concerning traumatic brain injuries and chronic traumatic encephalopathy (CTE) in the 1990s and 2000s.[54] Fortunately, wearable technology offers an opportunity for the NFL to atone for its wrongdoing: the NFL can partner with researchers and data analysts to further analyze research on head trauma and concussions in sports.[55] For years, the NFL and NCAA demonstrated reluctance to permit such research.[56] However, as leagues recognize their responsibility to alleviate the concussion crisis,[57] wearables—including concussion-tracking helmets—are becoming more ubiquitous.[58]

As the law develops in data collection and privacy, corporations and consumers—including professional sports leagues and athletes—must be flexible to adapt to uncertainty and volatility in rapidly changing innovations.[59]

---

[51] *Id.*

[52] Berman, *supra* note 25, at 544.

[53] Jason F. Arnold & Robert M. Sade, *Wearable Technologies in Collegiate Sports: The Ethics of Collecting Biometric Data from Student-Athletes*, AM. J. BIOETHICS J. 1, 2 (2017).

[54] *Id.*; *see also* Joe Ward et al., *111 N.F.L. Brains All But One Had C.T.E.*, N.Y. TIMES (July 25, 2017), https://www.nytimes.com/interactive/2017/07/25/sports/football/nfl-cte.html.

[55] Libby Plummer, *Super Bowl 50: How Wearable Tech Is Changing the NFL*, WAREABLE (Feb. 6, 2016), https://www.wareable.com/sport/super-bowl-2016-50-wearable-tech-in-the-nfl.

[56] Dennis Dodd, *NCAA Denies ACC Use of Helmet Cams, Sideline Communications*, CBS SPORTS (July 19, 2014, 8:23 AM), https://www.cbssports.com/college-football/news/ncaa-denies-acc-use-of-helmet-cams-sideline-communications/; David Butler II, *New Smart Helmet Could Spot Concussions in Real Time*, COLUM. MAG. (Winter 2018–19), https://magazine.columbia.edu/article/new-smart-helmet-could-spot-concussions-real-time.

[57] Alex Reimer, *Do NFL Fans Care About Player Safety*, FORBES (Jan. 12, 2016, 2:09 PM), https://www.forbes.com/sites/alexreimer/2016/01/12/nfl-tv-ratings-unaffected-by-violence/?sh=2ff204d811e5.

[58] Daniel Kaplan, *NFL to Continue Data Tracking in Helmets, Cleats and Mouthguards Amid COVID-19*, THE ATHLETIC (July 24, 2020), https://theathletic.com/1947836/2020/07/24/nfl-to-continue-data-tracking-in-helmets-cleats-and-mouthguards-amid-covid-19/.

[59] Kellogg, *supra* note 1, at 77.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.245 ● http://tlp.law.pitt.edu

III. WEARABLES IN COLLEGE SPORTS

College athletes are at an increased risk, relative to professional athletes, of inadequate biometric data protection. Without a representative union, student athletes have little control over policies governing wearable devices.[60] Further, under NCAA bylaws, student athletes are prohibited from receiving compensation from third parties' use of their names, images, and likenesses.[61] Courts generally maintain that "an individual college athlete's right of publicity is extraordinarily circumscribed and, in practical reality, nonexistent."[62] Of course, there are clear privacy distinctions between a college athlete's name and likeness being incorporated into a video game[63] versus his or her health data being made publicly available. Unless college athletes are given broader rights of publicity, they are at an increased risk of losing ownership of their biometric data.

Recent contracts between universities and apparel corporations are especially concerning in their lack of protection for student athlete data.[64] For example, a deal between the University of Michigan and Nike permits Nike to harvest data and "utilize" the information for undisclosed purposes.[65] While the contract stipulates that data collection must "be anonymous and comply with 'all applicable laws,'" such language will inadequately protect players' privacy.[66] Although Nike is not alone in its efforts to collect player data—Under Armour and Adidas have similar contracts requiring universities to use their biometric products[67]—it does appear to be ahead of its rivals.[68]

---

[60] Miller, *supra* note 12.

[61] NATIONAL COLLEGIATE ATHLETIC ASSOCIATION, 2020–21 NCAA DIVISION I MANUAL, § 12.4.1.1, https://web3.ncaa.org/lsdbi/reports/getReport/90008 ("Such compensation may not include any remuneration for value or utility that the student-athlete may have for the employer because of the publicity, reputation, fame or personal following that he or she has obtained because of athletics ability.").

[62] *In re* NCAA Student-Athlete Name & Likeness Licensing Litig., 724 F.3d 1268, 1289 (9th Cir. 2013).

[63] *Id.*

[64] Marc Tracy, *With Wearable Tech Deals, New Player Data Is Up for Grabs*, N.Y. TIMES (Sept. 9, 2016).

[65] *Id.*

[66] *Id.*

[67] Matthew Kish, *Nike's Expanded Effort to Collect Data from College Athletes Raises Privacy Concerns*, PORTLAND BUS. J. (Sept. 16, 2016, 10:55 AM), https://www.bizjournals.com/portland/news/2016/09/15/nikes-expanded-effort-to-collect-data-from-college.html.

[68] *Id.*

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.245 ● http://tlp.law.pitt.edu

The collection of this data may permit quicker treatment of athletes, but with student athlete biometrics being tracked as early as high school,[69] it is worth considering that parties collecting and storing data may be inclined to sell that information to the detriment of student athletes.[70] If it is the case that whomever collects the data maintains possessory rights, then high schools may sell information to universities, who may collect their own data and sell it to professional teams and leagues or third parties.[71] The inherent power imbalance between amateur athletes and universities further divides the two parties.[72]

IV. PROPOSALS FOR INCREASING ATHLETES' DATA PRIVACY PROTECTION

Some scholars believe that recent legal developments in the sports industry will spur the commercialization of wearables.[73] For example, the federalization of sports betting[74] incentivizes teams, leagues, casinos, television broadcasters, and other third parties to share in potential benefits.[75] Wearables may also make an impact on intellectual property law if players seek to license their likenesses in the form of biometric data.[76] With increased commercialization, athletes and leagues should give increased attention to privacy and ownership.

Ideally, the legislature will pass laws governing biometric data privacy.[77] In the meantime, athletes must consider that motivations to sell or misuse players' biometric data may outpace legal developments.[78] In both collegiate and professional sports, there are countless conflicts of interest pertaining to athletes' biometric data

[69] Ted Madden, *DeSoto High Using Wearable Technology to Get Better*, WFAA (Oct. 25, 2016), https://www.wfaa.com/article/sports/high-school/desoto-high-using-wearable-technology-to-get-better/287-341796370.

[70] Tracy, *supra* note 64.

[71] *Id.*

[72] Arnold & Sade, *supra* note 53, at 69.

[73] Berman, *supra* note 25, at 551–52.

[74] Murphy v. NCAA, 138 S. Ct. 1461, 1484–85 (2018) (holding that no federal law directly outlawed sports gambling, and that "Congress can regulate sports gambling directly, but if it elects not to do so, each [s]tate is free to act on its own").

[75] Berman, *supra* note 25, at 552.

[76] *Id.*

[77] Anthony Studnicka, *The Emergence of Wearable Technology and the Legal Implications for Athletes, Teams, Leagues and Other Sports Organizations Across Amateur and Professional Athletics*, 16 DEPAUL J. SPORTS L. & CONTEMP. PROBS. 195, 213 (2020).

[78] *Id.*

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.245 ● http://tlp.law.pitt.edu

and sports management.[79] Although contract negotiations and selling sensitive data are briefly addressed in some professional leagues' CBAs, there are other elements of biometric data ownership that could be problematic, including improper incentives to misuse or undermine players' data.[80] As such, organizations that collect, use, and store athletes' personal data should enact proactive measures to ensure privacy.

At a contractual level, leagues and players associations should extensively contemplate wearables and biometric data in future CBAs. As the wearable technology industry booms, it is important to proactively address potential future issues.[81] CBAs should be restructured in future negotiations with data security safeguards.[82] By including certain best practices in cybersecurity—for example, the National Institute of Standards and Technology's cybersecurity framework[83]—organizations can ensure adequacy in both internal and external security measures.[84]

Sports organizations and athletes should create a coalition to develop ethical, scientifically guided data collection standards.[85] The coalition could be composed of sports organization representatives, athletic representatives from all competition levels, data scientists, legislators, and legal scholars; such diversity would not only ensure equal and fair representation, but also the protection of college and amateur athletes who may be subject to biometric data collection.[86] The coalition may enact standards to ensure that research studies concerning wearables are publicly available and conform to best research practices.[87] For leagues and players, this may require partnering with third party research institutions to ensure conformity with ethical standards concerning data collection and privacy.[88]

---

[79] *Id.*

[80] *Id.*

[81] Joseph J. Lazzarotti, Mary T. Costigan & Ashley Solowan, *As Wearable Technology Booms, Sports and Athletic Organizations at all Levels Face Privacy Concerns*, NAT'L L. REV. (Apr. 5, 2019), https://www.natlawreview.com/article/wearable-technology-booms-sports-and-athletic-organizations-all-levels-face-privacy.

[82] Osborne & Cunningham, *supra* note 13, at 84.

[83] National Institute of Standards and Technology, *Cybersecurity Framework*, NAT'L INST. STANDARDS & TECH., https://www.nist.gov/cyberframework (last updated Mar. 15, 2021).

[84] Osborne & Cunningham, *supra* note 13, at 84.

[85] Arnold & Sade, *supra* note 53.

[86] *Id.*

[87] *Id.*

[88] *Id.*

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.245 ● http://tlp.law.pitt.edu

V. CONCLUSION

Fitness wearables are an incredible technological development for individuals, healthcare providers, and athletes alike. But it is important to recognize that biometric data derived from wearables is medical information that should be entitled to certain protections. Protecting data privacy is not a straightforward process, but athletes and sports organizations should work together to ensure best practices in data collection, storage, and management. By publicizing scientific research and creating a coalition that protects athletes' privacy interests, athletic organizations can proactively impact this booming industry.

Volume XXI – 2020-2021 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2021.245 ● http://tlp.law.pitt.edu