Journal of Legal Aspects of Sport, 2020, 30, 63 – 81
https://doi.org/10.18060/23894

Big Data, Big Problems: Analysis of Professional Sports Leagues' CBAs and Their Handling of Athlete Biometric Data

Sarah M. Brown and Natasha T. Brison*

The use and integration of wearable technology (wearables) into professional sports is increasing rapidly. At a minimum, the NFL, NBA, MLB, NHL, and MLS have all integrated wearables into their training. Teams' hope the biometric data obtained from the wearables will sharpen athletic performance, create competitive advantages, enhance fan experience, and generate new revenue streams. However, to obtain these desired outcomes leagues must adequately protect their athletes' biometric data (ABD). The purpose of this paper is to examine and compare the CBAs of the NFL, NBA, MLB, NHL, and MLS management of wearables and ABD. Specifically, this paper will discuss the potential gaps in protection of ABD within the CBA and explore whether federal and state laws are applicable to protect the data. Findings from this analysis improve our understanding of professional sport leagues management of ABD and expose the limitations of protection at the league, state, and federal level.

Keywords: wearable technology, professional sports, athlete biometric data, big data

Introduction

The North American sport market has seen strong, continual growth over the past decade and is projected to reach $78.53 billion by 2021.[1] As professional sport looks to keep growing and find additional ways to increase revenue, big data provides an opportunity to enhance fan engagement, create competitive advantages, and generate new revenue streams for leagues, teams, and athletes.[2] Specifically, big data generated from wearable technology (wearables), which

[1] Statista, *North America Sports Market Size from 2009 to 2021,* Statista.com, https://www.statista.com/statistics/214960/revenue-of-the-north-american-sports-market/, (last visited Oct. 1, 2018).

[2] Patterson Belknap Webb & Tyler, LLP, *Wearable Technology Fits into Professional Sports,* Lexology.com (2018), https://www.lexology.com/library/detail.aspx?g=2b1b620e-18b6-474e-8de4-cd0dd7556db8.

* Sarah M. Brown, JD, is a doctoral student in the sport management program in the Department of Health and Kinesiology at Texas A&M University; email: sarah_brown16@tamu.edu. Natasha T. Brison, JD, PhD, is an assistant professor of sport management in the Department of Health and Kinesiology at Texas A&M University; email: natasha.brison@tamu.edu.

collect various biometric statistics, including heartrate, skin temperature, and sleeping patterns, create additional information that can be packaged and delivered to consumers.[3] Wearables have become ubiquitous within the five major professional sport leagues in North America: the National Football League ("NFL"), National Basketball Association ("NBA"), National Hockey League ("NHL"), Major League Baseball ("MLB"), and Major League Soccer ("MLS"). At a minimum, each league has integrated wearables into athlete training, but the leagues' understanding and protection of the data is still very limited.[4] In order for professional sport to capitalize on the potential opportunities of athlete biometric data ("ABD"), the leagues must effectively manage ownership, access, privacy, and security of such data, as well as come to an agreement with their respective players' associations on suitable uses of the data. Appropriate league management and security is critical because ABD is an attractive commodity, and when put into a digitized format it can easily become susceptible to cyber threats, putting the athletes at risk of loss of privacy.

Thus, the purpose of this paper is to analyze and compare the protections for ABD set forth in the collective bargaining agreements ("CBAs") of the NFL, NBA, MLB, NHL, and MLS. Emphasis will be placed on examining the gaps in protection and potential athlete exposure, as well as the applicability of federal and state laws to biometric data collection. Part I presents a brief overview of the risks associated with the collection of professional ABD, specifically in connection with league management of the data. Part II focuses on applicable federal and state law, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and Genetic Information Nondiscrimination Act ("GINA") at the federal level, and Biometric Information Privacy Acts ("BIPA") at the individual state level. Part III analyzes each league's current administration of ABD, particularly investigating the CBA and its provisions regarding wearable technology. Finally, Part IV argues that a federal law is the most appropriate manner to provide uniform comprehensive protection for the collection of ABD

I. Potential Risks of ABD Collection

Biometric data is defined as "measurements or records that can be used to identify people as individuals; identifiers may be physiological (such as heartrate, temperature, and blood sample analysis) or behavioral."[5] The most sophisticated wearable devices can collect up to 1,000 data points per second.[6] With the accumulation of so much sensitive data, risk related to three entities must be evaluated: (1) the athlete whose data is being collected, (2) the entity

[3] Kristy Gale, *Data Generated by Wearable Technology Presents many Challenges in Sport,* Sport Techie (May 13, 2016), https://www.sporttechie.com/data-generated-by-wearable-tech-presents-many-challenges-in-sports/.

[4] Barbara Osborne, *Legal and Ethical Implications of Athletes' Biometric Data Collection in Professional Sport*, 28 Marq. Sport L. Rev. 37 (2017).

[5] Osborne, *supra* note 4, at 38.

[6] *Id*.

using the data, and (3) the vendor providing the wearable technology.[7] In this context, it is necessary to consider the athlete's right to privacy, the sport entity's obligation to manage and restrict access to the data and enact security protocols, and the vendor's duty to protect data stored on its databases and provide secured wearable devices.

Athlete privacy is a major issue with wearables, specifically, the risk of misappropriation of ABD. The nature of a professional athlete's work requires some surrendering of personal privacy, including health information, but data collected from wearable technology represents a departure from the standard health information obtained from an athlete's physical exam.[8] For example, wearables collect data including players movements, muscle fatigue, exertion, and speed whereas measurements taken during a physical exam are limited to weight, height, and body temperature. Moreover, physical exams are generally limited to once a year, whereas wearables are continuously collecting the athlete's data. The leagues differ in when the players wear the wearables, but at a minimum players are wearing the technology every practice. Therefore, the data being collected is not only more intimate and personal, but it is being collected on a regular basis. This continual collection of data then allows for the athlete's performance and effort level to be constantly compared, creating a risk for the athlete—a risk that did not exist when athletes were simply given a physical exam at the beginning of each season.

Wearable technology enables access to intimate, sensitive data, particularly an athlete's physiological analytics, and without clear delineation of ownership and the athlete's ability to restrict others' access, an athlete's privacy is at risk because the athlete has no control over the data. Of particular concern are the wearables that athletes wear 24 hours a day, in which GPS is tracking the athlete's location. This type of data goes beyond the athlete's health and training and into the athlete's private life. Therefore, it is critical for there to be a clear understanding of the intended purpose(s) of the data collection. For example, data collected from wearables has the potential to create a disadvantage for players during contract negotiations and could even cut short their playing careers if, for instance, certain data revealed a player violated team conduct rules.[9] Moreover, unwanted disclosures could impact endorsements and other monetary opportunities, both during and after an athlete's career.[10]

Another area of trepidation is the security, including storage, of the data collected. Both the sport team and the wearable technology company are obligated to secure ABD from unauthorized access and use.[11] Data hacking and leaked information through unauthorized disclosures are a serious issue in professional sport. For example, former St. Louis Cardinal scouting director Chris Correa

---

[7] Brian Lam, *Athletes and Their Biometric Data—Who Owns It and How It Can Be Used,* JDSUPRA.COM (Dec. 20, 2017), https://www.jdsupra.com/legalnews/athletes-and-their-biometric-data-who-96340/.

[8] Ryan H. Purcell & Karen S. Rommelfanger, *Biometric Tracking from Professional Athletes to Consumers,* 17 Am. J. of Bioethics, 72, 73 (2017).

[9] Karkazis, *supra* note 5, at 46.

[10] *Id*. at 52.

[11] *Id*. at 53.

illegally accessed the Houston Astros' player personnel database and is currently serving a 46-month prison sentence for corporate espionage.[12] Also, prior to the 2016 Summer Olympics, the World Anti-Doping Agency's athlete database was hacked and U.S. athletes' personal medical information was leaked.[13] These examples demonstrate the susceptibility and desirability for access to digitized athlete data. Further, temptation to hack these databases may be even greater since the U.S. Supreme Court issued a ruling to legalize sport betting in 2018.[14] Wearables generate 1,000 data points a second, data that fantasy football players would love to have access to and utilize in their decision-making.[15] Further, cybercriminals who steal ABD from unsecured databases now have more opportunities to make legal bets and earn profit off of the misappropriated information.[16] Therefore, the teams and wearable vendors must enact and uphold strict security standards for access and data storage. This is important at the team and vendor level, as there are few regulations or laws governing the use of biometric devices in professional sport.[17]

II. Applicable Federal and State Law

Since professional athletes are categorized as employees, they are afforded protections under federal and state employment regulations, including the Genetic Information Nondiscrimination Act. GINA was enacted to combat employers from gaining access to employee genetic information and using that information in discriminatory practices.[18] GINA states:

> It shall be an unlawful employment practice for an employment agency—(1) to fail or refuse to refer for employment, or otherwise to discriminate against, any individual because of genetic information with respect to the individual; (2) to limit, segregate, or classify individuals or fail or refuse to refer for employment any individual in any way that would deprive or tend to deprive any individual of employment

---

[12] Mike Axisa, *We Now Know Extent of Cardinals Hack and the Unprecedented Penalties from the MLB,* CBSSPORT.COM (Jan. 30, 2017), https://www.cbssport.com/mlb/news/we-now-know-extent-of-cardinals-hack-and-the-unprecedented-penalties-from-mlb/.

[13] Rebecca R. Ruiz, *Russian Hackers Leak US Athletes Medical Records,* BOSTON GLOBE (Sept. 14, 2016), https://www.bostonglobe.com/sport/olympics2016/2016/09/14/russian-hackers-leak-athletes-medical-records/AfnrZ4WRQqseuxOtUFZ4hO/story.html.

[14] *See generally,* Murphy v. Nat'l Collegiate Athletic Ass'n., 138 S.Ct. 1461 (2018) (this ruling repealed the Professional and Amateur Sports Protection Act (PASPA), which prohibited state-sanctioned sports betting).

[15] Chris Smith, *How Wearable Tech is Bringing Real Data to a Fantasy Football World,* WAREABLE.COM (June 29, 2017), https://www.wareable.com/wearable-tech/wearables-and-future-of-fantasy-football-230.

[16] Zachary Zagger, *Sports Teams Must Tackle Hacking Risk Amid Legal Gambling,* LAW360 (Sept. 24, 2018), http://www.law360.com/articles/1085391/print?section=sport.

[17] Karkazis & Fishman, *supra* note 5, at 47.

[18] Tiffany Lee, *Biometrics and Disability Rights: Legal Compliance in Biometric Identification Programs,* 2 ILLINOIS J. OF LAW AND TECH., 209, 223 (2016).

> opportunities, or otherwise adversely affect the status of the individual as an employee, because of genetic information with respect to the individual; or (3) to cause or attempt to cause an employer to discriminate against an individual in violation of this title.[19]

The breadth of GINA could potentially encompass a team's use of ABD and restrict the team's ability to use such information in contract negotiations. However, the act is limited to genetic information, which wearable technology does not currently monitor or collect. Despite wearables currently not measuring genetic information, some professional sports teams, like the New York Giants, blood test their players to identify biomarkers in order to improve performance.[20] As the technology continues to develop, it may start to measure this type of information and GINA will likely come into play and help provide protections to athletes who do not enjoy such protections under their leagues' current CBA.

Additionally, athletes may look to HIPAA for protections because presently, no federal law exists to specifically address biometric data collection.[21] HIPAA does regulate some biometric data, but there is ambiguity in what information is protected due to multiple definitions of biometric data, and athletes may sign waivers that exempt teams from having to comply with federal requirements.[22] HIPAA is structured to allow employees, or in this case players, to waive many privacy measures and disclosure restrictions imposed by HIPAA.[23] Further, the Department of Health and Human Services ("DHHS"), the entity that enforces HIPAA, has stated that professional sport teams are not likely entities that would need to comply with HIPAA privacy rules.[24] Moreover, ABD may be deemed part of employment records and therefore fall out of HIPAA protection.

Although there is currently no federal legislation dedicated to biometric data, three states have enacted statutes aimed at protecting individuals' right to privacy as it relates to their biometric data. Specifically, Illinois, Texas, and Washington have all enacted legislation aimed at protecting the collection and use of biometric data. [25] The statutes are applicable to private entities, including

---

[19] Genetic Information Nondiscrimination Act of 2008 § 2(4).

[20] Nikole Tower, *Who Is Monitoring Data from Wearable Technology,* GLOBALSPORTMATTERS.COM (Sept. 11, 2018), Retrieved from https://globalsportmatters.com/science/2018/09/11/who-is-monitoring-data-from-wearable-technology/.

[21] Osborne, *supra* note 6, at 46.

[22] *Id*.

[23] *Id*.at 52

[24] *Id*. at 52.

[25] Todd Kennard, Brandy Ranjan & Jackson Lavelle, *Biometric Data in the Workplace Could Trigger Privacy Litigation Wave,* JONESDAY.COM (Nov. 2017). Retrieved from https://www.jonesday.com/files/Publication/c5c46c73-ce02-4bc6-83e3-0dcd58b6a2ef/Presentation/PublicationAttachment/d0b347d6-a1cc-4106-9898-1faf8e03a11f/Biometric%20Data%20in%20the%20Workplace.pdf.

professional sport teams.[26] Generally, these laws impose conditions on disclosing, securing, collecting, and using biometric data, and provide a mechanism for private right of action or enforcement by state attorneys general.[27] In fact, both the MLB and NBA CBA provisions, in regards to wearables, are similar to the regulations imposed by the Illinois BIPA. The CBAs and statute both require disclosure of what information is being collected, why the data is being collected, execution of a waiver or release, prohibition on commercial use of the data, and requirement to treat and protect such data as confidential information.[28] Sport teams based in Illinois, Texas, and Washington should consider their obligations under their respective BIPA to ensure compliance and avoid potential punitive penalties, particularly those sport teams in the NFL, MLS, and NHL whose CBAs barely, if at all, address wearable technology. Although, as the Illinois and Texas statutes currently read, their definition of biometric data does not include the data collected by wearable technology. Rather, these state statutes are geared towards data such as fingerprints and retina scans. A major reason for this is because the statutes were enacted in 2008, before wearable technology became used as prominently. However, the state of Washington's statute, which was enacted in 2017, will likely be applicable to biometric data collected from wearables.

III. The Collective Bargaining Agreements

While the potential risks of ABD collection exist and legislation is limited, all four parties—leagues, athletes, teams, and wearable technology companies—have a vested interest in protecting the ABD. Given the novelty of the technology and relatively limited understanding of wearables as a resource, leagues are still developing management and security protocols for the data through their CBAs.

CBAs are the agreements reached between a league's owners and their respective players' union and serve as the primary governing authority for the relationship between players and their respective teams. The CBAs establish specific operational elements of the league, including revenue sharing, salary cap, disciplinary rules, and general regulations of the league.[29] Additionally, CBAs are the key source for a professional league's management and protection of ABD collection. For that reason, it is critical for each players' union to completely understand the risks associated with the collection of ABD and to ensure necessary protections are negotiated into current or future CBAs.

---

[26] Mintz.com, *Athletes and Their Biometric Data—Who Owns It and How Can It Be Used,* MINTZ.COM (Dec. 19, 2017), Retrieved from https://www.mintz.com/insights-center/viewpoints/2017-12-athletes-and-their-biometric-data-who-owns-it-and-how-it-can-be.

[27] Kennard, *supra* note 59.

[28] Nicholas Zych, *Collection and Ownership of Minor league Athlete Activity Biometric Data by Major League Baseball Franchises,* 14 DEPAUL J. OF SPORT L. 129, 136 (2018).

[29] Brittany Forgues, *Collective Bargaining Agreements and What Has Changed in the NBA and NFL,* MSLAW.EDU, (April 2012), http://www.mslaw.edu/verdict-3/.

A. National Basketball Association CBA

The NBA CBA was negotiated in 2016 and went into effect in July 2017. These CBA negotiations occurred after the growth of wearable technology and both the league and players association wanted to outline a set of rules governing the use of wearables. The NBA is one of two professional leagues that discusses wearable technology at length in its current CBA, but the language is far from a comprehensive management plan for ABD collection. The three-page section in the CBA prohibits wearables from in-game use and outlines regulations and restrictions of wearables in practice.[30] Teams may ask a player to use a league-approved device in practice, on a voluntary basis, to collect ABD in which he will have access. Furthermore, the team must provide each player with a written, confidential letter explaining what is being measured, what the measurements mean, and the benefits of collecting ABD.[31] However, and most importantly, the CBA bans use of the data in contract negotiations with a penalty of a $250,000 fine if data is used, and creates a committee (wearable committee) to approve wearable devices for player use and to set cyber security standards.[32] However, security protocols have not been incorporated into the CBA. It is imperative to have such protocols memorialized into the CBA to ensure proper governance and protection. Without a uniform standard in place, teams may adopt different security requirements, which could result in varying levels of protection for athletes. The wearable committee is a joint advisory committee made up of three representatives appointed by the NBA and three representatives appointed by the National Basketball Association Players Association ("NBAPA").[33] At least one of the three appointed individuals from both sides must have at least three years of experience in sport medicine with the NBA or a Division I collegiate basketball program, and none of the committee members can have a financial interest in a company that produces or sells wearable technology.[34] Additionally, the CBA allows for the parties to continue discussions, in good faith, about the commercialization of ABD.[35] The parties' agreement to continue negotiations after the effective date of the CBA demonstrates awareness of the opportunity for monetizing ABD while also understanding the complexity behind such opportunities.

On its face, the CBA appears to provide a complete outline of the applicability of wearable technology in the NBA, but there is still ambiguity around

---

[30] Jeremy Venook, *The Upcoming Privacy Battle over Wearables in the NBA,* THEATLANTIC.COM, (April 10, 2017), https://www.theatlantic.com/business/archive/2017/04/biometric-tracking-sport/522222/.

[31] Dusan Johnson, *NBA Says No to In-Game Use of Wearable Technology,* (Feb. 1, 2017), https://gadgetsandwearables.com/2017/02/01/nba-wearable-technology/.

[32] National Basketball Association, *Article XXII, Section 13* (2017) archived at https://cosmic-s3.imgix.net/3c7a0a50-8e11-11e9-875d-3d44e94ae33f-2017-NBA-NBPA-Collective-Bargaining-Agreement.pdf.

[33] *Id*.

[34] *Id*.

[35] *Id*. at section 13(i).

ownership. There are also no explicit security protocols or guidelines for storing and handling ABD, and no right of action for an athlete if his data is misappropriated. In particular, Section 13(h) states:

> [A] player will have full access to all data collected on him from approved Wearables. Members of the Team's staff may also have access to such data, but it can be used only for limited purposes as set forth below. Data collected from a Wearable worn at the request of a Team may be used for player health and performance purposes and Team on-court tactics and strategic purposes only.[36]

While this section discusses athletes' and others' access, it is silent on ownership of the data. It is critical to establish ownership, especially when it comes to the commercialization of ABD because ownership gives control over if and how ABD can be commercialized. Also, NBA athletes only have the right to access data and not restrict the list of individuals who have access. Currently, the team's staff has access to the data, but the staff includes myriad individuals.[37] If athletes had the ability to restrict access, it may help alleviate the fear of coaches and staff using biometrics in contract negotiations, as well as potential unwanted disclosures. Despite the CBA banning use of data in contract negotiations, it will likely be difficult to prove such information was used to influence negotiations or trades. Additionally, it is unclear whether an athlete can wear a league-approved device during practice without the data automatically being sent to the team. For example, an athlete may want to wear a device for his own personal training and not share the information with his respective team. Furthermore, the CBA needs to include a mechanism for athletes to bring claims if their data is misappropriated due to the negligence of the league or team. Without such a provision, the player has no remedy under the CBA if his ABD is wrongfully misappropriated.

B. Major League Baseball CBA

The MLB CBA is relatively new, going into effect in 2017.[38] Its inclusion of a wearables section is not surprising because wearable technology has been used in a limited capacity in the MLB since 2016.[39] Since then, the league has approved four devices: the Motus sleeve (biomechanics sleeve), the Zephyr bioharness (measures heart rate and breathing), Catapult (GPS locator), and the WHOOP (measures heart rate, sleep data, and temperature).[40] The CBA allows players to wear the devices in-game. While teams and players are not permitted to access the data during games, the data is available immediately

[36] *Id*. at Section 13(h).

[37] *Id*.

[38] Major League Baseball Collective Bargaining Agreement,

Attachment 56 (2017) archived at http://www.mlbplayers.com/pdf9/5450407.pdf.

[39] Venook, *supra* note 19.

[40] Stephanie Springer, *An Update on Wearable Baseball Technology,* (Aug. 7, 2018), https://www.fangraphs.com/tht/an-update-on-wearable-technology/.

afterward.[41] MLB players' use of wearables is strictly voluntary, and prior to any player agreeing to use a wearable device, the team must provide the player with a written description of the technology and a list of individuals who will have access to the data collected.[42]

The CBA provides for the creation of a Joint Committee on Wearable Technology ("JCWT"), comprised of four members: two appointed by the Major League Baseball Players Association ("MLBPA") and two appointed by the Office of the Commissioner.[43] The purpose of the committee is to review potential use of wearables in games or during pre-game activities, and advise the Playing Rules Committee ("PRC") on whether to approve such technology. The JCWT meets biannually to discuss potential issues relating to player safety, data management, privacy, confidentiality, and other relevant topics.[44] This provision is vital for the safeguarding of players' data, as the JCWT monitors issues and has the ability to address potential problems regularly, rather than waiting and reacting to issues as they occur. Additionally, the CBA explicitly states that all data collected will be treated as highly confidential and will not become part of a player's medical record.[45] This statement is an interesting caveat because information collected in the course of providing healthcare may be protected under federal, state, and common law.[46] However, by not classifying the ABD as part of an athlete's medical record, it could help avoid unwanted disclosures of player health information that are required by law.

The CBA also allows for players to request their respective team to restrict the list of individuals who have access to the data and destroy such data at any time. However, it is important to note that teams are not compelled to restrict the list of individuals who have access to the data but are compelled to delete the data when requested to do so by the athlete. Therefore, athletes are given some control of their data, which can reduce the risk of loss of privacy and unwanted disclosure. However, the CBA also allows for players to be monitored away from the ballpark, where all the data that was being collected during practice and in-game is still being collected while the player is at home. This creates new privacy concerns because the collected data is no longer part of the player's work. For example, wearable technology has GPS tracking, so players' whereabouts can be monitored all day/night. This type of monitoring is a clear loss of an athlete's autonomy and invasion of his privacy. Despite players having some control of the data, the type of data being collected in MLB may cross the line from health and performance to personal lifestyle.

Lastly, the CBA clearly prohibits commercial use or exploitation of a player's data by a team, MLB, or any entity related to MLB. It is unclear, however, whether exploitation of player data includes use of such information in contract

41 *Id*.

42 *Id*. at para. 4.

43 *Id*. at para. 7.

44 *Id*.

45 *Id*. at para. 4.

46 Osborne, *supra* note 4, at 50.

negotiations. The ambiguity in this language could cause significant issues in contract negotiations for an athlete whose biometric data may put him at a disadvantage. For instance, a team may attempt to leverage heart rate fluctuations or stamina issues as recorded by the wearables during negotiations to demonstrate that the player is not in top physical shape.

While the CBA is silent on ownership of the data, it appears that athletes have some control of the collected data, but without specification of ownership, athletes are unable to use the data for commercial opportunities. Specifying ownership is extremely important for decisions on management of ABD. Further, the CBA is also lacking specific security protocols and guidelines for the protection of ABD, as well as a mechanism for athletes to bring claims for unwanted ABD disclosures. These two major gaps in protection may leave ABD exposed to potential cyber threats and athletes with no reprieve if their data has been compromised due to negligence by the league or their team.

C. The National Football League CBA

The NFL CBA was signed in 2011 and is set to expire after the 2020 season. The current CBA went into effect before wearable technology was used in the NFL. In fact, Zebra Technologies, a company that specializes in marking, tracking, and computer printing technologies, did not start providing the NFL with their sensors to track players' movements until 2014.[47] The current NFL CBA discusses the use of sensors on player equipment during games and practices for the purposes of collecting information regarding performance and movement, as well as medical and other player safety-related data.[48] Specifically, the language states,

> The NFL may require all NFL players to wear during games and practices equipment that contains sensors or other nonobtrusive tracking devices for purposes of collecting information regarding performance of NFL games, including players' performance and movements, as well as, medical and other player safety-related data. Sensors shall not be placed on helmets without the NFLPA's [National Football League Players Association] consent. Before using sensors for health or medical purposes, the NFL shall obtain the NFLPA's consent. [49]

Other than this brief paragraph, there is no mention of sensors, wearable technology, or ABD collection in the CBA. The NFL's ephemeral mention of ABD collection is worrisome, because there is no explicit understanding of management, use, ownership, access, or security protocols of the data, despite teams actively using wearable technology with their athletes. Given the NFL's injury types and the heavy nature of statistics utilized, it is an ideal match-up with

---

47 Tom Taylor, *NFL Technology: What's New for the 2017 Season,* (Aug. 30, 2017). Retrieved from, https://www.si.com/nfl/2017/08/30/nfl-technology-whats-new-2017-season.

48 National Football League Collective Bargaining Agreement, Article 51, Section 13(c) (2011). Archived at https://nfllabor.files.wordpress.com/2010/01/collective-bargaining-agreement-2011-2020.pdf.

49 *Id*.

wearable technology. For example, Seattle-based startup Vicis, in collaboration with the University of Washington, has developed a helmet designed to combat concussions.[50] Also, Catapult Sport, a sport technology company, has partnered with 25% of the NFL franchises to monitor players' performance.[51] Specifically, Catapult's OptimEye S5, which sits between the player's shoulder blades, measures energy exertion and tracks speed and distance.[52] This data is particularly helpful for coaches who can see in real time whether a player is performing at his full ability. However, with teams having unrestricted access to the data, players are at a disadvantage, as the data now alerts personnel on an athlete's limitations or lack of effort. Additionally, without specific security guidelines, the collected data may not be properly secured, leaving ABD exposed to potential misappropriation and exploitation.

The NFLPA, via its athlete-driven accelerator, the OneTeam Collective, established a partnership with WHOOP, a human performance company, to collect ABD with wearables.[53] The NFLPA is the first and only players' association to independently partner with a wearable technology company, with no obligation to share the information with the NFL and its teams.[54] Specifically, this partnership provides players easy access and ownership of their data, while also allowing the opportunity to commercialize the data through the NFLPA's group licensing program.[55] The WHOOP Strap 2.0 was distributed to every player at the start of the 2017 season, except to the players who chose to opt out of the program. The terms of this partnership assist in alleviating pressure points around players' privacy, especially since WHOOP devices monitor the athletes 24/7. The continuous monitoring of data encroaches into players' personal lives outside of football and could potentially collect intimate details, such as a player's sex life.[56] Since the players have ownership and ultimate control of the data, there is less of a concern about misappropriated use and unwarranted access. However, the NFLPA and WHOOP both need to ensure that sufficient security protocols are in place to protect the athletes' data from cyber threats.

Despite the NFLPA having its own agreement with WHOOP and the NFLPA giving athletes control of the collected data, this does not alleviate the risks associated with the NFL's collection of data through sensors or other wearable

---

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

[51] *Id*.

[52] Hugh Langley, *Catapult's Tech Is Giving the NFL its Moneyball Moment*, (Jan. 26, 2017). Retrieved from https://www.wareable.com/sport/catapult-nfl-optimeye-tracking-senior-bowl-7557.

[53] NFLPA. *WHOOP Strikes Landmark Deal as the Officially Licensed Recovery Wearable of the NFL Players Association,* NFLPA.COM (April, 24, 2017). Retrieved from https://www.nflpa.com/players/news/whoop-strikes-landmark-deal-as-the-officially-licensed-recovery-wearable-of-the-nfl-players-association.

[54] *Id*.

[55] *Id*.

[56] Alex Schultz, *Why Is This Wearable-Tech Company Helping College Teams Track How Often Athletes Sleep, Drink, and Have Sex?* DEADSPIN, (April 12, 2017). Retrieved from https://deadspin.com/why-is-this-wearable-tech-company-helping-college-teams-1794218363.

technology used by individual teams. Since the NFL and individual teams are actively collecting players' data, the CBA must address ownership, use, management, privacy, and security of the data. Further, the CBA needs to detail the purpose(s) of data collection and what personnel will have access to ABD. As the NFL progresses and seeks to implement more technology, it will be interesting to see how the NFLPA handles the negotiations surrounding these issues. As of now, the NFLPA has taken the lead on wearable technology, leaving the NFL as a hopeful consumer of its own athletes' commercialized data. It is important to note, if NFL players chose to commercialize their data and sell it to the NFL, they will need to add restrictions into the purchase agreement to prohibit use of the data in contract negotiations.

D. National Hockey League CBA

The NHL CBA, which was signed in 2013, does not mention the use of wearable technology or any athlete tracking device. However, the use of wearables is a topic on the minds of both the league and the players association. NHL commissioner Gary Bettman hopes that tracking athletes will enhance fan engagement and provide a complete story by adding supplemental statistics to games, such as speed of a player's shot or skating, while the National Hockey League Players Association ("NHLPA") is concerned with how this data will be used, specifically whether it will be considered in contract negotiations. [57] The executive director of the NHLPA stated that when it comes to data concerning the players' health, "the biometric data is player-personal, health-related and in our view, owned [by the players]."[58]

Despite wearable technology missing from the CBA and the NHLPA's reluctance to give the league its players' biometric data, multiple NHL teams have being using wearables for training and during practices for the last three years.[59] In fact, it is commonplace for NHL teams to have their players wear devices that monitor their velocity and muscle usage.[60] For example, the Buffalo Sabres and Philadelphia Flyers use Catapult OptimEye S5 to monitor their athletes' movements.[61] The NHLPA seems comfortable with allowing its players' biometric data to be collected in practices and training, but is unwilling to cross the line into in-game action.

Although the NHLPA has made it clear that wearing devices in-games is off the table (at least for now), athlete data is still being collected and therefore raises serious concerns. The use of wearable technology by NHL teams and the lack of a governing provision in the CBA creates a legal quagmire, as there

[57] Greg Wyshynski, *Player Tracking Coming to the NHL? It's Complicated*, FORBES.COM (Feb. 28, 2018). Retrieved from https://www.forbes.com/sites/darrenheitner/2013/08/14/questions-concerning-copyright-of-athlete-tattoos-has-companies-scrambling/#1ec1553c4a21.

[58] *Id*.

[59] *Id*.

[60] *Id*.

[61] Matthias Neuner, *Wearables for Icehockey,* WEARABLETECHNOLOGIES.COM, Retrieved Nov. 29, 2018, from https://www.wearable-technologies.com/2016/09/wearables-for-icehockey/.

is no delineation on ownership, access, use, privacy, or security protocols. For example, if team personnel have access to ABD, which it appears they do, there are no restrictions in place to keep teams from using the data in contract or trade negotiations. Further, there are no standardized security protocols for protecting the athlete data from cyber threats. Therefore, it would be advantageous for the NHLPA to negotiate the use, ownership, management, and security of ABD in its next CBA or request that the current CBA be amended to include such provisions.

E. Major League Soccer CBA

In 2012, adidas announced that MLS teams will use its miCoach Elite System, a fitness tracking device that measures players' movements, speed, heart rate, and power output, starting in the 2013 season.[62] Additionally, adidas created a miCoach tab and application (app) on the adidas soccer Facebook page that gave fans access to real-time player statistics during the 2012 All-Star game.[63] This type of access is great for fan engagement, but the then-current MLS CBA did not have provisions managing the disclosure of the athletes' data. Furthermore, individual teams like Real Salt Lake have used Wahoo's TICKR X to monitor its players during the offseason to ensure they are working out and will be fit and injury-free by the start of the season.[64] While this type of tracking has been successful for Real Salt Lake, it invades athletes' personal lives and raises several privacy issues.[65]

MLS negotiated its most recent CBA in 2015, and the highest priority for both the league and its players' association was the collection and information sharing of medical data.[66] Despite the mutual sentiment of importance, the new CBA only has one clause dedicated to teams' use of wearable technology. Section 9.10 of the CBA states that the league may require its athletes to wear a monitoring device in connection with training and in games (if the device is found not to impede performance), and allows for MLS teams to collect ABD, including exertion rate, and such data is shared with the coaching staff, technical director, and other relevant team, league, United States Soccer Federation, and Canadian Soccer Association personnel.[67] Further, the CBA permits the league to publicly

---

[62] Jill Duff, *ADIDAS Technology to Track Major League Soccer Players*, PCMAG.COM (July 19, 2012). Retrieved from http://www.pcmag.com/article2/0,2817,2407383,00.asp.

[63] *Id*.

[64] Phillip Tracy, *One of Major League Soccer's Best Teams Adopts Player Tracking Technology,* SPORTTECHIE.COM (May 4, 2015). Retrieved from https://www.sporttechie.com/one-of-major-league-soccers-best-teams-adopts-player-tracking-technology/.

[65] *Id*.

[66] Taylor Soper, *Technology 'Part of the DNA' for Major League Soccer, Commissioner Says on Eve of Geekwire Sport Tech Summit*, GEEKWIRE.COM (July 12, 2016). Retrieved from https://www.geekwire.com/2016/technology-part-dna-major-league-soccer-commissioner-says-eve-geekwire-sport-tech-summit/.

[67] *MLS Collective Bargaining Agreement Ratified and Signed*, MLS, art. 9.10 (Feb. 1, 2015) [hereinafter MLS CBA], https://s3.amazonaws.com/mlspa/Collective-Bargaining-Agreement-February-1-2015.pdf?mtime=20180213190926

disclose performance measures or metrics that are based off of athlete physiological testing without the players' union consent. As the agreement stands, the league does need to conduct a dialogue with the players' union to notify the association that they plan on publicly disseminating the data.

The standard of care towards ABD in MLS is extremely worrisome, as the league and individual teams are actively collecting athletes' data without uniform rules, regulations, limitations, and security protocols. Additionally, the league's arbitrary control over certain performance metrics being publicly disseminated without the players' union consent is a major breach in athletes' privacy because the athlete cannot control what information the league disseminates to the public. While the league hopes to use wearable technology and real-time player statistics to engage its fans, it comes at a steep price to the athletes who are sacrificing not only privacy, but potential monetary gains. For example, the CBA does not place any restrictions on how the league or team can use the data. Thus, players' data may be used against them during contract negotiations or cause to cut players from the team. Of particular concern is the lack of homogeneity among teams, where some individual teams mandate that players wear monitoring devices out of season and/or during practices so team trainers can assess their fitness level, while other teams do not have such requirements.[68] Lastly, without uniform security protocols or confidentiality of the players' data, there is a risk of security breach. The players' union must negotiate these key issues in the next CBA to help afford its athletes the necessary precautions for management of ABD.

F. Similarities and Differences Among the Professional Leagues' CBAs

As discussed in the previous sections, the professional leagues' CBAs are all at various stages with management of wearables and ABD, with the MLB and NBA providing the most robust language and the NHL providing no wearable language at all. Table 1 compares each league's controlling provisions for wearables or ABD collection by breaking the language out into eight categories: (1) management, (2) use, (3) ownership, (4) privacy, (5) access, (6) security, (7) commercial use, and (8) definition. These categories were chosen because they represent the highest areas of concern for athletes with the integration of wearable technology into professional sport. [69] This comparison is important, as it demonstrates how each league is handling critical aspects of ABD protection and reveals gaps in the current protections.

---

[68] Lauren Hepler, *The Quantified All-Star: How Wearable Tech Is Changing the Way Pro Sport Are Played, Paid for and Watched,* BIZJOURNALS.COM (Aug. 8, 2014). Retrieved from https://www.bizjournals.com/sanjose/feature/biz-of-sport/2014/the-quantified-athlete-how-wearable-tech-gets-the.html.

[69] Venook, *supra* note 18; Karkazis & Fishman, *supra* note 5

Table 1. Comparison of Wearables Governing Provisions in the Professional Leagues' CBAs

	MLB	NBA	NFL	NHL	MLS
Management	Team must provide an explanation of the technology proposed. Playing Rules Committee (PRC) has the authority to approve use and devices. Wearable committee created and will meet biannually to discuss topics related to wearable technology.	Team must provide an explanation of what the device will measure, what those measurements mean, and the benefits to the player for obtaining such data. Wearable committee created to establish security protocols, review and approve requests for wearable devices.	N/A	N/A	N/A
Use	Voluntary; only approved devices. In practice and in game. Medical and performance.	Voluntary; only approved devices. In practice only. Medical, on-court strategic decisions, and performance.	Players may be required to wear sensors In practice and in game. Medical and performance.	N/A	Players may be required to wear a monitoring device in connection with training.
Ownership	N/A	N/A	N/A	N/A	N/A
Privacy	Wearable data is treated as highly confidential; not part of player's medical record.	N/A	N/A	N/A	Performance measures may be publicly disseminated, without the Union's approval.
Access	Player (direct access); Team (listed personnel). Player may request to restrict others access.	Player (full access); Team staff (full access).	N/A	N/A	Team shares results with player.
Security	At player request, data is destroyed.	Wearable committee sets cybersecurity standards. Teams security standards approved by the wearable committee.	N/A	N/A	N/A
Commercial Use	Commercial use is strictly prohibited.	Wearable data may not be leveraged in contract negotiations; violation is a $250,000 fine. Continue discussions in good faith about commercialized data.	N/A	N/A	N/A
Definition	Any device designed to collect and/or analyze data related to a player's health or performance.	Measures movement information, biometric information, or other health, fitness, and performance information.	N/A	N/A	Physiological testing.

IV. Recommendation for Managing ABD at a Federal Level

Wearable technology is the new age of professional sport and if the leagues want to capitalize on opportunities from the technology, there needs to be adequate, uniform protection. Uniform protection is imperative considering the recent ruling in *Murphy v. National Collegiate Athletic Association,* which repealed the Professional and Amateur Sport Protection Act ("PASPA"), a federal law prohibiting state-sanctioned sport gambling.[70] With PASPA being overturned, sport gamblers will want access to ABD to make more educated betting decisions. Further, the NFL, NHL, NBA, and MLB all have partnerships with sport betting companies.[71] As a result, a standardized federal law will be beneficial in ensuring homogeneous protection for athletes in all of the major professional leagues. In other words, by adopting a federal regulation to manage ABD collection, athletes, no matter what sport they play, will all enjoy the same level of protection. For example, MLS players' data will be treated the same as NFL players' despite the popularity disparity between the two leagues. A federal statute is the best means to manage and protect against these potential risks, cyber hacking, because individuals can be held accountable under a federal statute for misappropriating or stealing ABD, whereas they cannot be held accountability under CBA rules, which are only applicable to the parties of the CBA. Further, if each league was responsible for enacting their own protections, it could be a multi-year process and will likely not have the same level of protection that a federal statute can offer. For instance, a federal statute can implement harsh penalties, much like we see in the European Union's ("EU") General Data Protection Regulation ("GDPR"), for the leagues, individuals, teams, and wearable technology companies, whatever entity is not fulfilling their obligations. A CBA, meanwhile, would likely not impose such harsh penalties. Moreover, collegiate athletes' biometric data is being collected as part of their training.[72] Universities are collecting a massive amount of data on their student-athletes, including heart rate, glucose level, strain, and fatigue.[73] This data, alone or in the aggregate, can reveal potential sensitive personal information relating to an athlete's identity, as well as impact coaching

---

[70] 138 S.Ct. 1461 (2018).

[71] Wayne Parry, *US Sport Leagues Split on How to Monetize Sports Betting,* APNEWS.COM (Feb. 4, 2019). Retrieved from https://www.apnews.com/86888142961d45a191cf00d1f026f302; *see also,* Lucas Thomas, *NFL Completes U-Turn on Sports Betting as League Prepares to Seek Casino Sponsor.* CASINO.ORG (Dec. 12, 2018), Retrieved from https://www.casino.org/news/nfl-likely-to-join-other-pro-sports-leagues-in-finding-casino-partner; REUTERS, *Major League Baseball and Fanduel Strike Sports Betting Deal.* CNBC.COM (Aug. 15, 2019). Retrieved from https://www.cnbc.com/2019/08/15/major-league-baseball-and-fanduel-strike-sports-betting-deal.html.

[72] Joseph Lazzarotti, Mary Costigan & Ashley Solowan, *As Wearable Technology Booms, Sports and Athletic Organizations at all Levels Face Privacy Concerns.* JACKSONLEWIS.COM, https://www.workplaceprivacyreport.com/2019/04/articles/health-information-technology/as-wearable-technology-booms-sports-and-athletic-organizations-at-all-levels-face-privacy-concerns/ (last visited July 8, 2019).

[73] *Id*.

decisions such as playing time and scholarship opportunities.[74] Unfortunately, student-athletes do not have the bargaining power of professional athletes or potential protections extending from a CBA. Without a comprehensive federal regulation of biometric data, both student-athletes and professional athletes are at risk of loss of autonomy and privacy.

The U.S. should look to the EU's GDPR, which addresses biometric data in detail and provides uniform requirements for ABD protection in EU member states.[75] The GDPR represents a groundbreaking piece of legislation geared towards data privacy.

The GDPR replaced the Data Protection Directive ("DPD"), which was enacted in 1995.[76] The aim of the GDPR is to "balance the innovative capabilities that biometrics provides and organizations' obligation to collect that data responsibly and keep it secure."[77] The GDPR defines biometric data in broad terms as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person."[78] This expansive definition is necessary to keep up with the growth and evolution of biometric technology and to ensure that future types of biometric data are included in the GDPR's protections. Under the GDPR, biometric data is considered sensitive data, meaning there are specific guidelines and regulations for processing and protecting the data, including obtaining consent from the individual whose data is being collected.[79] Additionally, the GDPR requires data controllers to conduct a privacy impact assessment to determine whether processing the data will likely result in high risks to the rights of the individual whose data is being collected.[80] The GDPR will impact sport teams that track ABD; specifically, sport organizations are subject to steep fines up to 4% of the organization's worldwide revenue if the data is not managed per GDPR's guidelines. As wearable use continues to grow and become more ingrained into the professional sport, the need for a uniform federal law is imminent. Such federal law should include the following: (i) a broad definition for ABD, (ii) classify ABD as confidential and sensitive, (iii) consideration of the potential risks related to ABD, and (iv) significant fines for noncompliance.

---

[74] *Id*.

[75] Luke Irwin, *GDRP: Things to Consider when Processing Biometric Data* (Sept. 15, 2017). Retrieved from https://www.itgovernance.eu/blog/en/gdpr-things-to-consider-when-processing-biometric-data.

[76] Sophie Goodman, *A Game Changer in the Personal Data Protection in the EU,* Mich. St. U. Int'l L. Rev. (Jan. 29, 2018). Retrieved from https://www.msuilr.org/msuilr-legalforum-blogs/2018/2/19/a-game-changer-in-the-personal-data-protection-in-the-eu.

[77] Irwin, *supra* note 71.

[78] Regulation (EU) 2016/679 General Data Protection Regulation. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[79] Danny Ross, *Processing Biometric Data? Be Careful under the GDPR,* iapp.org (Oct. 31, 2017). Retrieved from https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/.

[80] *Id*.

Another piece of legislation the U.S. government can use as a guideline is the California Consumer Privacy Act of 2018, Cal. Civ Code §§ 1798.110 *et seq*. ("CCPA"). This act requires U.S. companies to implement similar privacy initiatives as those outlined in the GDPR, to afford California residents unparalleled data privacy rights. Additionally, the act's definition of personal information specifically includes biometric information. The CCPA went into effect January 1, 2020. While the CCPA represents a step toward protecting individuals' privacy rights, a federal regulation is more appropriate. Similar to the GDPR, which not only raised the bar for personal-data privacy and security, but also set a consistent level across all member states, a federal regulation can raise the bar and set a consistent level across all states. Moreover, given the structure of the U.S., it can authorize agencies such as the Federal Trade Commission and state attorneys general to enforce the law, unlike the GDPR, which relies on agencies in each of the member states for enforcement.[81] A strong federal law would provide all Americans, in addition to professional athletes, with a standard of protection of their personal information and the knowledge that their personal information is being handled in ways that are consistent with their interests.[82]

V. Conclusion

Despite current use of wearables in all five professional leagues, there are still serious gaps in protection of ABD. Even the NBA and MLB, whose CBAs contain the most extensive provisions, are missing key elements, including explicit security protocols, delineation of ownership, and a mechanism for athletes to bring claims for misappropriated ABD. The NFL, NHL, and MLS have failed to appropriately contemplate management and use of ABD in their respective CBAs. While some states have started to enact their own statutes aimed at the protection of ABD, there is currently no applicable federal law. Therefore, the leagues, teams, and players cannot depend on state or federal laws for protection. Instead, each players' association must negotiate the necessary protections into the CBA. Most importantly, each league's players' association should negotiate athlete ownership of ABD to help lessen risk of issues around privacy and commercialization of data. As the owners of ABD, athletes will be able to restrict or deny access, and be the decision-maker for how and if their ABD is commercialized. Further, players' associations should seek out advice and counsel from experts in digital technology to help create specific security protocols to be incorporated into the CBA, as well as into any agreements leagues enter into with wearable technology providers. Lastly, since wearable technology is rapidly evolving, it is necessary for players' associations to negotiate a right to amend the CBA to keep abreast with technological changes, as well as update security and privacy protocols, which is already done biannually in

[81] Cameron F. Kerry. *A Federal Privacy Law Could do Better than California's,* LATIMES.COM (April 25, 2019), https://www.latimes.com/opinion/op-ed/la-oe-kerry-ccpa-data-privacy-laws-20190425-story.html.

[82] *Id*.

MLB. Wearable technology provides numerous opportunities for enhanced fan engagement, safer training for athletes, and commercialization. The protection of ABD is critical to the realization of these opportunities.