Dalhousie Journal of Legal Studies

Volume 28 Article 28

1-1-2019

# Moneyball in the Era of Biometrics: Who Has Ownership Rights Over the Biometric Data of Professional Athletes?

Christopher Casher

Follow this and additional works at: https://digitalcommons.schulichlaw.dal.ca/djls

 Part of the Entertainment, Arts, and Sports Law Commons, Health Law and Policy Commons, and the Privacy Law Commons

This work is licensed under a Creative Commons Attribution 4.0 License.

## Recommended Citation

Christopher Casher, "Moneyball in the Era of Biometrics: Who Has Ownership Rights Over the Biometric Data of Professional Athletes?" (2019) 28 Dal J Leg Stud 1.

This Article is brought to you for free and open access by the Journals at Schulich Law Scholars. It has been accepted for inclusion in Dalhousie Journal of Legal Studies by an authorized editor of Schulich Law Scholars. For more information, please contact hannah.steeves@dal.ca.

# *MONEYBALL* IN THE ERA OF BIOMETRICS: WHO HAS OWNERSHIP OVER THE BIOMETRIC DATA OF PROFESSIONAL ATHLETES?

**Christopher Casher***

**ABSTRACT**

The 2003 release of Michael Lewis's book, *Moneyball,* brought into the mainstream a new paradigm for professional sports management: the use of statistical analysis to identify currently undervalued athletes in an effort to gain a competitive advantage. This pressure to accurately value athletes has led, in part, to the widespread collection of professional athletes' biometric data. While biometric data can create many benefits, its misuse can lead to detrimental outcomes for the athletes, including inequitable contract negotiations, loss of potential revenue from monetization of said data, and a loss of privacy. Thus, this paper seeks to determine who holds the ownership rights over biometric data collected from professional athletes. I argue that the question of ownership is unanswered by the collective bargaining agreements and standard player contracts for professional sports leagues in North America, as well as by the *Personal Health Information Protection Act* and the *Personal Information Protection and Electronic Documents Act*. I turn to the precedent set by the Supreme Court of Canada regarding ownership of patient medical records to conclude that ownership rights over the biometric data belong to the party collecting such data, and not the athletes themselves. Nevertheless, the collective bargaining agreements and relevant legislation afford athletes some protections against the misuse of their biometric data.

**Citation:** (2019) 28 Dal J Leg Stud 1.

* Christopher Casher is completing his articles at the law firm Fasken Martineau DuMoulin LLP in Toronto, ON and will be called to the Ontario Bar in 2019. He is a graduate of the Schulich School of Law at Dalhousie University and of Queen's University, where he completed a BA (Hons) in Political Studies and Economics with distinction. He is grateful to Alexis Muscat and the DJLS team for their editing assistance, and for organizing the Think Tank 6 Student Research Prize.

# INTRODUCTION

In many ways, the discussions surrounding professional sports in North America would be almost unrecognizable to the average fan 20 years ago. Each Sunday, cameras capture quarterbacks and coaches staring at tablet computers on the sidelines, studying previous drives. The debate over the National Basketball Association's (NBA) Most Valuable Player Award has fans comparing newly popularized statistics such as player efficiency rating, true shooting percentage, and points per possession.[1] Major League Baseball (MLB) teams advertise openings for sabermetrics analysts in their front offices.[2] Each development represents an evolution to the paradigms that have traditionally governed sports management. Among these evolutions is the collection and analysis of biometric data.

The adoption of new technologies has resulted in major changes within professional sports. As so often happens, this development in technology has occurred faster than the law can adapt, creating questions around use and regulation. Among these, who holds the ownership rights to the biometric data of professional athletes gathered from wearable devices in games and in practice? What regulations, if any, currently exist for the collection, use, and disclosure of this data? I seek to answer these questions in this paper. I will begin by exploring the context in which the development of biometric tracking in sports arose, considering the current rise of the use of analytics in professional sports. Next, I will define the term biometric data, examine how it is being utilized in professional sports, and identify the harms that may arise from its unregulated use. I will then explore the implications of contract law, labour law, applicable legislation, case law and explore any existing regulations to answer the question of ownership over biometric data.

To aid in this analysis, I will employ certain parameters and presumptions. To begin, the research for this paper has been conducted from the perspective of

---

[1] Basketball Reference, "Calculating Individual Offensive and Defensive Ratings" (last visited 9 April 2018), online: *Basketball Reference* < https://www.basketball-reference.com/about/ratings.html>.

[2] Ben Lindbergh & Rob Arthur, "Statheads Are The Best Free Agent Bargains In Baseball", *FiveThirtyEight* (26 April 2016), online: <https://fivethirtyeight.com/features/statheads-are-the-best-free-agent-bargains-in-baseball/>.

a professional athlete who is a resident of Ontario, playing for a private sports organization located in Ontario. Thus, relevant provincial and federal legislation has been considered. Further, this athlete is presumed to have signed the relevant standard form contract provided for within the respective collective bargaining agreements (CBAs). The fact that four of the five major professional sports leagues are located in the United States raises jurisdictional questions as to the application of Canadian law over certain athletes. Conclusions to these questions are inherently factually specific, and thus beyond the scope of this paper, which attempts to conduct an environmental scan of this issue rather than suggest practical application. However, I have attempted to address these questions where relevant. Further, it is possible that the question of data ownership can be addressed through private contract clauses either between the team and the athlete, or between the team and the company providing biometric tracking technology. Given this limitation, I instead seek to consider the legal influences beyond a clause in a private player contract that will either supplement situations where a contract is silent on the issue of biometric data ownership, or, potentially supersede one that is not.

From the perspective of this hypothetical professional athlete, I will analyze the three major sources of legal influence over the relationship between the athlete and their team to determine the question of ownership rights. First, I will explore the CBAs entered into between the players' unions and the respective North American sports leagues to determine whether the question of ownership has already been negotiated. Next, I will analyze applicable provincial and federal legislation to determine if the legislature has addressed this question. Finally, I will delve into the relevant and analogous case law to determine if the courts have addressed the question of ownership. Based on this analysis, I conclude that the precedent set by the Supreme Court of Canada regarding ownership of patient medical records suggests that the biometric data collected from professional athletes belongs to the party that collected such data, and not the athletes themselves.

## THE RISE OF SPORTS ANALYTICS

Professional sports teams operate in a marketplace, with regulations intended to both level the playing field and to increase competitiveness within the league. A salary cap limiting what teams can spend on athlete salaries exists to address the resource imbalance between large and small market teams. The athlete drafting process, which is designed to put the worst performing teams in the best position to sign the most talented incoming athletes, helps address talent imbalances. Further, teams have to be selective with the athletes they sign, as CBAs impose limitations on the number of active athletes each team can have. Thus, teams are under great pressure to properly evaluate each athlete's abilities, so as to maximize the success of the team while minimizing costs. To meet this pressure, teams utilize analytics (the analysis of athlete performance data) to influence athlete management decisions.[3]

As long as professional teams have competed for championships, management has utilized some form of analytics to evaluate athletes.[4] What has changed over time are the metrics used to evaluate athletes, the technology used to obtain these metrics, and how these metrics are interpreted.

The practice of using statistical analysis to influence management decisions was relatively marginal until the 2003 release of Michael Lewis's best seller, *Moneyball*, after which the practice was popularized and began to become legitimized by league executives across MLB.[5] The release of this book was such a watershed moment that its title, *Moneyball*, is still used today to refer to the application of statistical methods on athlete performance, regardless of the sport in question.[6] The logic behind *Moneyball* is quite simple; through statistical

---

[3] Benjamin Baumer & Andrew Zimbalist, *The Sabermetric Revolution: Assessing the Growth of Analytics in Baseball* (Philadelphia: University of Pennsylvania Press, 2014) at 11, 30.

[4] The demand for the analytical evaluation of incoming athletes is well demonstrated through the National Football League's (NFL) scouting "combine", wherein college football athletes who have declared for the draft are evaluated on certain drills which teams believe to be indicative of an athlete's potential. This event began in the 1980's, when teams lacked the resources needed to properly evaluate athletes from across the country. Even though this resource gap has largely been eliminated, the persistence of the scouting "combine" indicates the NFL's demand for analytics. For more on this topic, see Kevin Clark, "The NFL Combine Has a Usefulness Problem" (26 February 2016), online: *The Wall Street Journal* <https://www.wsj.com/articles/the-nfl-combine-has-a-usefulness-problem-1456533621>.

[5] Baumer, *supra* note 3 at 1, 12, and 90.

[6] *Ibid* at 11, 17, and 27.

analysis, management can identify undervalued athletes to gain a competitive advantage. While Lewis was successful in telling the story of the 2002 Oakland Athletics, his success also began to erode the competitive advantage upon which the team's success was based.[7] This has led to a continuous search for new metrics by which teams can identify undervalued athletes. As discussed in greater detail below, it is this pressure for a new competitive advantage which has, in part, not only led to teams collecting biometric data, but has also created the incentive to misuse this data to the athletes' detriment.

## BIOMETRIC DATA

### Defining the Term

Instead of tracking an athlete's in-game performance, biometric data measures the performance of an athlete's body during the game. The term "biometric data" has a broad definition, referring to the measurement and tracking of physical and physiological characteristics. This information has many potential uses, but in relation to sports and athletics it is mainly used to assess the performance and recovery of athletes.[8] The physical and physiological characteristics measured varies depending on the specific technology used, and the purpose it is being used for, however, these measurement possibilities will only increase as the technology continues to develop. While mainstream biometric trackers today are limited to measurements from sensors placed on the skin, industry insiders predict that more invasive sensors, either ingested or implanted, with the ability to measure a greater amount of data are not far off the horizon.[9] Given that the use of this technology will only increase, it is important to consider basic legal questions early in its development.

Currently, biometric trackers function by placing wireless sensors on athletes' bodies, which in turn relay the data collected in real time to hand-held computers and tablets. These devices then use proprietary software to interpret

[7] *Ibid* at 37.
[8] Katrina Karkazis & Jennifer R Fishman, "Tracking US Professional Athletes: The Ethics of Biometric Technologies" (2017) 17:1 American J Bioethics 45 at 45-46.
[9] *Ibid* at 47.

the data based upon the team's needs.[10] We can look to the services advertised by one of the industry leaders, STATSports to illustrate to potential of biometric data collection. While the services advertised are not necessarily indicative of the true capabilities of the product, a brief summary demonstrates what services are available in the market.

On its website, STATSports tailors its advertisements to its product's usefulness in individual sports. Under American football, it advertises that its wearable devices track over 50 metrics. These metrics vary from the athlete's running speed and distance to more advanced metrics such as the reaction time and acceleration after the snap and the impact received. Through the collection of enough data, STATSports advertises that its product will learn each athlete's individual level of conditioning and understand how close each athlete is to full exertion. It also advertises that its product can assist by detecting how much an athlete has recovered from injuries by using metrics such as "left vs right foot impacts …[which] can give coaches and athletic trainers data showing whether a rehabilitating athlete is putting more force through his healthy side and therefore going easy on the injured leg. Coaches can see whether or not a athlete is fully ready to return."[11] Other metrics advertised for basketball include heart rate exertion, acceleration, explosive distance and a fatigue index.[12] These advertised metrics demonstrate how these companies take the basic physiological measurements, and use software to interpret the data in a method tailored to the needs of the targeted sport.

## Use and Potential Misuse in Professional Sports

Ostensibly, teams use biometric monitoring devices to both assist athletes in avoiding injury (by preventing overexertion) and to monitor injury recovery.[13] By tracking athletes' biometric statistics in real-time, teams can better understand how athletes are recovering from their games, practices, and workouts, identify

---

[10] *Ibid* at 45.
[11] STATSports, "Football", online: <http://statsports.com/football/>.
[12] STATSports, "Basketball", online: <http://statsports.com/basketball/>.
[13] Natalie Weiner, "Goal Line Lasers, Football Sensors and More: Why the NFL Is Slow to New Tech", *Bleacher Report* (29 January 2018), online: <http://bleacherreport.com/articles/2756568-goal-line-lasers-football-sensors-and-more-why-the-nfl-is-slow-to-new-tech>.

which athletes are at risk of injuring themselves, and adjust the athlete's environment accordingly.[14]

This understanding of the way teams use biometric data, however, is naïve to say the least. There are too many incentives and too much opportunity for this data to be used to benefit the parties in power at the athletes' expense. Two of the main harms that can arise from the misuse of biometric data are inequitable outcomes in contract negotiations, and an athlete's loss of privacy rights.

Given the substantial salary the average professional athlete now earns, it may be difficult to comprehend how their contract negotiations can be considered inequitable. For clarity, I am not suggesting that these harms reach the level of unjust enrichment, or that they would make the execution of these contracts unconscionable. Certainly, the presence of agents on behalf of the athletes and the processes outlined in the CBAs would severely inhibit these arguments. Instead, I argue that asymmetric access to the athlete's biometric data can result in inequitable outcomes for future contracts.[15]

Athletes represent significant investments for a team, financially and in terms of the opportunity-cost the athlete's spot on the roster takes.[16] A team is therefore incentivised to have as much data as possible on its athletes, which includes biometric data. Inequity can arise, however, when the use of the data is masked, or if the data itself is inaccurate. With the ever-increasing amount of data available to team managers, it is almost inevitable for this data to influence contract negotiations.[17] This influence can become inequitable to the athlete if he or she is unaware of the data's influence, resulting in teams negotiating lower contracts on the basis of information that the athlete may not have access to. Masking the data is not difficult to do. If there is an athlete who is often out too late and whose sleep trackers indicate a lack of sleep, management might refer to them as having bad character. An athlete who does not have a high enough heart rate during certain drills in practice can be painted as lacking effort. If an athlete has low oxygen intake during sprints, the team may write them off as having low

[14] Jeremy Venook, "The Upcoming Privacy Battle Over Wearables in the NBA", *The Atlantic* (10 April 2017), online: <https://www.theatlantic.com/business/archive/2017/04/biometric-tracking-sports/522222/>.
[15] Black's Law Dictionary, 10th ed, sub verbo "inequity."
[16] Venook, *supra* note 14.
[17] Ibid.

endurance.[18] Whether or not the biometric data is a fair representation of athletic qualities, not informing the athlete of the data underlying these qualifications can put them at a disadvantage.

The above problem assumes that the devices collecting the data are accurate and are being used for their proper purpose. However, many of these devices use various algorithms to simplify the complex factors recorded. As Karkazis and Fishman note in their article on the subject, "[when] thinking about the utility of an algorithm, it is not simply a question of whether it is the right algorithm for the job, but whether a concept like athlete recovery can ever be captured by an algorithm."[19] Further, there is the risk that those interpreting the data may not understand what the data represents. Team management can conflate the process with the result, separating the data from the performance it is intended to beget.[20]

Another example showing how biometric data can be used to harm an athlete's interest is found in the terms of the standard player contracts in the CBAs of each league. Each contract contains a clause that is substantially similar to this one, taken from the National Hockey League (NHL) player contract, wherein the player covenants "to keep himself in good physical condition at all times during the season," with the potential for the athlete's contract to be terminated if this representation is not upheld.[21] Previously, these clauses were interpreted subjectively. Now, biometric data captured from athletes can make the interpretation of these clauses more objective in determining what is to be considered "good physical condition," without the athlete necessarily knowing what the objective standard is that they are required to meet, or how the data will be used in this interpretation.[22]

Another set of potential harms from the use of biometric data is the potential for breaches of the athlete's privacy interests. As one legal commentator noted, "unlike previous advances in analytics, biometric data provides

---

[18] Ibid.
[19] Karzakis, *supra* note 8 at 49.
[20] Venook, *supra* note 14.
[21] "Collective Bargaining Agreement between NHL and NHLPA, September 16, 2012 – September 15, 2022", online (pdf): *NHLPA* <https://www.nhlpa.com/the-pa/cba> at Exhibit 1, s 2(b) [NHL-NHLPA Agreement].
[22] Karzakis, *supra* note 8 at 50.

information about the basic mechanics of a player's body that is [not] available to the naked eye, or even the high-tech-camera-enhanced eye."[23] This data has inherent privacy interests associated with it, and thus issues of disclosure are especially concerning. Athletes have an inherent interest in determining who has the ability to access their biometric data, an interest that is more difficult to protect without ownership rights over the data. Further, even with strong storage and disclosure procedures in place, there is a real risk that this data can still be leaked to the public.[24] Various groups, such as fans and fantasy sports participants, looking to get a competitive advantage and who have obvious interests in obtaining the data, increase this risk. The potential market for this information, coupled with the innate privacy interests associated with the data, have led many to argue that if this biometric data can be monetized, it should be the athletes, and not the teams, who benefit from this monetization.[25]

## COLLECTIVE BARGAINING AGREEMENTS

In each of the major North American sports leagues, the relationship between the athletes and their teams are governed by CBAs negotiated between the various athletes' unions and their respective leagues. Players unions have strongly advocated with the leagues to negotiate CBAs that respect and protect the interests of the athletes. It is likely that the collection and use of biometric data will be included in the CBAs, given the potential harms identified with the practice. If the CBA directly addresses the issue of biometric data ownership, or if the assignment of the data's ownership can be reasonably read into an existing clause, then the ownership rights will clearly be determined.

As previously noted, I am conducting this review through the lens of Ontario law, contrary to the choice of law clauses present in many of the CBAs. Addressing this potential conflict of laws, while beyond the scope of this paper, is also not necessary to determine the question I seek to answer. A simple textual interpretation of the CBAs reveals that ownership rights over biometric data have

[23] Venook, *supra* note 14.
[24] Ibid.
[25] Karzakis, *supra* note 8 at 57.

not been explicitly negotiated for in any CBA or standard player contract and helps develop our understanding of the legal landscape surrounding biometric data collection.

### Direct Reference to Biometric Data

Upon reviewing the CBAs for five professional sports leagues in North America, only two make a direct reference to biometric data. The five CBAs included are for the National Football League (NFL), NBA, MLB, NHL, and the CFL:

| CBA | Years Effective | Direct Reference to Biometric Data |
|---|---|---|
| NFL – NFLPA[26] | 2011-2020 | Not included |
| NHL – NHLPA[27] | 2012-2022 | Not included |
| CFL – CFLPA[28] | 2014-2018 | Not included |
| NBA – NBPA[29] | 2017-2024 | Included |
| MLB – MLBPA[30] | 2017-2021 | Included |

Only the most recently negotiated CBAs explicitly mention biometric data and trackers, while those negotiated only a few years earlier are silent on the issue. As will be discussed, while the NFL's CBA does reference wearable sensors on athletes, it does not contain any explicit reference to biometric data, nor does it provide for any substantial regulations on the collection, use, or disclosure of the data. This pattern demonstrates that the issue of tracking and recording biometric data has only recently become a priority for professional athletes.

---

[26] "Collective Bargaining Agreement", 2011, online (pdf): *NFL Communications* <https://nfllabor.files.wordpress.com/2010/01/collective-bargaining-agreement-2011-2020.pdf> [NFL-NFLPA Agreement].
[27] NHL-NHLPA Agreement, *supra* note 21.
[28] "Collective Bargaining 2014-2018", online (pdf): *CFLPA* <https://cflpa.com/download/collective-bargaining-agreement-2014-2018/> [CFL-CFLPA Agreement].
[29] "2017 NBA-NBPA Collective Bargaining Agreement", online (pdf): *NBPA* <https://nbpa.com/cba/> [NBA-NBPA Agreement].
[30] "2017-2021 Basic Agreement", online (pdf): *Major League Baseball Players* <http://www.mlbplayers.com/pdf9/5450407.pdf> [MLB-MLBPA Agreement].

### *National Basketball Association*

The current CBA between the NBA and the National Basketball Players Association (NBPA) came into effect July 1, 2017, and contains a comprehensive set of regulations for the use of biometric trackers by athletes.[31] While these regulations protect the athletes from many of the potential harms arising from misuse of the biometric data, the CBA does not directly assign ownership rights to the biometric data collected. Even though the question of ownership is left unanswered, a review of the rights and regulations negotiated for in the CBA is instructive in demonstrating the athletes' concerns regarding biometric data.

These regulations are in section 13 of Article XXII "Player Health & Wellness," and give a broad definition to "wearables", defining them as a device that measures movement, biometric, health, fitness and performance information.[32] The first part of this section creates a Joint Advisory Committee on "wearables" with three members each from the NBA and NBPA, none of who are allowed to have any interest in a "wearables" company. This Joint Advisory Committee has two functions: to review requests for approval of wearable devices submitted by teams, the NBA, or NBPA, and to set cyber security standards for the storage of data collected.[33] The requests are evaluated for accuracy and potential harm to athletes, and teams cannot request athletes to use any device until it has received approval.[34] Devices that were already in use before the agreement are temporarily grandfathered in, until the Joint Advisory Committee is able to review the devices and the data security standards in place.[35] The section then goes on to set out standards and restrictions on the use of biometric tracking devices by teams. While teams may request an athlete to use an approved device, such use is voluntary, and a team's request must be accompanied by a written explanation of "(i) what the device will measure, (ii) what each such measurement means; and (iii) the benefits to the athlete in obtaining such data."[36] Therefore, NBA athletes will be fully informed of the data

---

[31] NBA-NBPA Agreement, *supra* note 29 at art XXII s 13, art XXXIX s 1.
[32] *Ibid* at art XXII s 13(a).
[33] *Ibid* at art XXII s 13(c).
[34] *Ibid* at art XXII ss 13(c), 13(e).
[35] *Ibid* at art XXII s 13(f).
[36] *Ibid* at art XXII s 13(g).

collected about them before they agree to their use, directly addressing the root issue of many potential inequitable outcomes between the team and the athletes.

This CBA also contemplates some of the potential harms from the misuse of this data identified earlier. Athletes are given full access to all of their data, and the data cannot be used to influence contract or trade negotiations, with teams liable for fines up to $250,000 for violations.[37] These provisions, while potentially hard to enforce, directly address the potential for teams to engage in bad-faith bargaining. The CBA also prohibits the data from being made public or used for any commercial purpose.[38] This prohibition recognizes the commercial nature of this information, as it protects athletes by preventing the team or the NBA from capitalizing on athlete data and instead compels the parties to continue to negotiate for the commercialization of said data.[39] Overall, the CBA between the NBA and NBPA provides a comprehensive regulatory regime for the implementation of biometric tracking devices that protects the economic, privacy, and safety interests of the athletes.

***Major League Baseball***

The current CBA between the MLB and the Major League Baseball Players Association (MLBPA) came into effect December 1, 2016, and runs until December 1, 2021.[40] Similar to the NBA's CBA, the agreement contains a section detailing the "approval, use and implementation of wearable technology" that collects biometric data, and sets out regulations designed to safeguard the athletes from the teams' misuse of this data.[41] Another similarity the agreement shares with the NBA's CBA is that it too does not directly assign the ownership rights to the biometric data collected. A review of the MLB's CBA illustrates the concerns the MLBPA had while negotiating the agreement, and how these concerns contrast to those negotiated for by the NBPA.

In the agreement, wearable technology is given a broad definition, referring to "any equipment, program, software, device or attire which is designed to

---

[37] *Ibid* at art XXII s 13(h).
[38] *Ibid* at art XXII s 13(i).
[39] Ibid.
[40] MLB-MLBPA Agreement, *supra* note 30 at art XXVI.
[41] MLB-MLBPA Agreement, *supra* note 30 at Attachment 56.

collect and/or analyze information or data related to [an athlete's] health or performance at any location (including on-field, off-field and/or away from the ballpark)."[42] Not only does this definition capture the devices contemplated by this paper, but it also includes devices that would be assigned by teams to take measurements of the athletes off the field. The inclusion of this broad definition is a proactive move by the MLBPA, as the issue of off-field measurements is very likely to be contentious. Already, in 2015, the NFLPA filed a grievance against the NFL for teams mandating the use of sleep monitoring devices on their athletes without the approval of the NFLPA.[43]

The agreement between the MLB and MLBPA follows a similar structure to the NBA's CBA in regard to regulating biometric tracking devices. The existing Playing Rules Committee must approve all wearable technology before an athlete can use it.[44] To assist in the approval process, the agreement creates a Joint Committee on Wearable Technology, with members from both the MLB and the MLBPA, to review applications for new wearable technologies and to provide the Playing Rules Committee with recommendations.[45] Unlike the NBA's CBA, however, the agreement does not contain guidelines or standards for the Committee to base its decision on.

The agreement gives the athletes a great deal of agency regarding the use and implementation of biometric tracking devices and demonstrates a great concern for the privacy rights of the athletes. The use of these devices is strictly voluntary, and teams must provide athletes with a written explanation of the technology being proposed, as well as a list of every person who will have access to the data collected.[46] The agreement limits this list to eight identified positions within team management, and gives the athlete the ability to restrict or expand this list.[47] The biometric data collected is to be treated as highly confidential, even after the expiration of the agreement.[48] It does not become part of the athlete's

[42] *Ibid* at Attachment 56, s1.
[43] Tom Pelissero, "NFLPA files grievance over sleep monitoring devices being used by teams", *USA Today* (22 October 2015), online: <https://www.usatoday.com/story/sports/nfl/2015/10/22/nflpa-nfl-sleep-monitors/74402474/>.
[44]MLB-MLBPA Agreement, *supra* note 30 at Attachment 56, s 6.
[45] *Ibid* at s 7.
[46] *Ibid* at ss 2, 3.
[47] *Ibid* at s 4.
[48] Ibid.

medical record, and therefore will not be available to a new team if he is traded.[49] Further, the athlete has the ability to request a copy of all of the data the team has collected, as well as to request that the team delete the data at any point.[50]

While the agreement demonstrates a strong concern for the athlete's privacy, when compared to the NBA's CBA it contains relatively little protection on how the data will be used by teams, thus doing less to prevent many of the inequitable outcomes contemplated earlier. The only explicit limitation on teams and the league is that any commercial use or exploitation of the data is prohibited.[51] While this potentially leaves open the opportunity for athletes themselves to benefit commercially from the data, it likely does not provide athletes with protections from the potential inequitable outcomes in contract and trades negotiations identified earlier.

### *National Football League*

The current CBA between the NFL and the National Football League Players Association (NFLPA) came into effect in 2011, making it the oldest CBA to reference wearable technology and sensors.[52] Unlike the NBA and MLB agreements, however, it is clear upon reviewing the NFL's CBA that the section was not intended to provide comprehensive regulation over the use of wearable biometric trackers, instead leaving those details to be negotiated by the parties later. Given the sparse detail in the section, it is unsurprising that the agreement also does not assign the ownership rights to the data collected.

The sub-section dealing with sensors, tucked away under the section "On-Field Microphones and Sensors", itself under the article titled "Miscellaneous," applies to "sensors or other non-obtrusive tracking devices," and divides these into two categories based on their purpose.[53] Those that are used for health and medical purposes of athletes can only be implemented after the NFL receives the NFLPA's consent.[54] While the agreement gives no criteria by which the NFLPA will evaluate proposals, the NFLPA did release a form titled "Sensor Technology

---

[49] Ibid.
[50] *Ibid* at ss 3, 4.
[51] *Ibid* at s 5.
[52] NFL-NFLPA Agreement, *supra* note 26 at xiv.
[53] *Ibid* at art 51, s 13.
[54] Ibid.

CBA Compliance Form" in the 2015 preseason.[55] While this form is private, it can be presumed to include some requirements by which the NFLPA would evaluate proposals by teams. The agreement also contemplates sensors implemented to collect information about the athlete's performance and movement during NFL games. The agreement gives the NFL the ability to require athletes to wear these sensors, except for those placed on the athletes' helmets, which still require the consent of the NFLPA.[56]

While the agreement lists a set of procedures intended to protect athletes from the misuse of in-game audio recordings captured under the section, it is silent on the teams' and the league's intended use of the personal health data collected by these wearable sensors.[57] Thus, while the NFLPA may be able to negotiate regulations separately, as it stands the CBA does little to protect the athletes from the potential harms identified earlier.

### Reading-in Ownership Rights

The current CBA between the NFL and the National Football League Players Association (NFLPA) came into effect in 2011, making it the oldest CBA to reference wearable technology and sensors.[58] Unlike the NBA and MLB agreements, however, it is clear upon reviewing the NFL's CBA that the section was not intended to provide comprehensive regulation over the use of wearable biometric trackers, instead leaving those details to be negotiated by the parties later. Given the sparse detail in the section, it is unsurprising that the agreement also does not assign the ownership rights to the data collected.

The sub-section dealing with sensors, tucked away under the section "On-Field Microphones and Sensors", itself under the article titled "Miscellaneous," applies to "sensors or other non-obtrusive tracking devices," and divides these into two categories based on their purpose.[59] Those that are used for health and medical purposes of athletes can only be implemented after the NFL receives the

---

[55] Pelissero, *supra* note 43.
[56] NFL-NFLPA Agreement, *supra* note 26 at art 51, s 13(c).
[57] Ibid.
[58] NFL-NFLPA Agreement, *supra* note 26 at xiv.
[59] *Ibid* at art 51, s 13.

NFLPA's consent.[60] While the agreement gives no criteria by which the NFLPA will evaluate proposals, the NFLPA did release a form titled "Sensor Technology CBA Compliance Form" in the 2015 preseason.[61] While this form is private, it can be presumed to include some requirements by which the NFLPA would evaluate proposals by teams. The agreement also contemplates sensors implemented to collect information about the athlete's performance and movement during NFL games. The agreement gives the NFL the ability to require athletes to wear these sensors, except for those placed on the athletes' helmets, which still require the consent of the NFLPA.[62]

While the agreement lists a set of procedures intended to protect athletes from the misuse of in-game audio recordings captured under the section, it is silent on the teams' and the league's intended use of the personal health data collected by these wearable sensors.[63] Thus, while the NFLPA may be able to negotiate regulations separately, as it stands the CBA does little to protect the athletes from the potential harms identified earlier.

## LEGISLATION

Since the question of biometric data ownership is not answered, either directly or indirectly, by the CBAs, the next consideration is whether applicable legislation dictates the assignment of ownership rights. As mentioned, this analysis is from the perspective of a professional athlete who plays in, and is a resident of, Ontario. Thus, both Ontario and federal legislation is potentially applicable to this athlete and must be reviewed. The two pieces of legislation that are potentially applicable and will be analyzed are the *Personal Health Information Protection Act* and the *Personal Information Protection and Electronic Documents Act*.[64]

---

[60] Ibid.
[61] Pelissero, *supra* note 43.
[62] NFL-NFLPA Agreement, *supra* note 26 at art 51, s 13(c).
[63] Ibid.
[64] SO 2004, c3 [*PHIPA*]; SC 2000, c5 [*PIPEDA*].

## The Personal Health Information Protection Act

The *Personal Health Information Protection Act (PHIPA)* was passed by the Ontario Legislature in 2004 in recognition of the sensitive nature of health information, and in an effort to balance the privacy interests of individuals with the operational needs of those in the healthcare system.[65] Similar to the CBAs explored earlier, *PHIPA* sets out rules for the collection, use, and disclosure of personal health information by health care practitioners, and gives individuals a right to access their own personal health information.[66] *PHIPA* also obligates those who hold the personal health information to correct any inaccuracies that are brought to their attention.[67] Before examining these obligations further, first we must determine whether *PHIPA* is applicable to a private sports organization based in Ontario that mandates athletes to wear biometric trackers.

### *Applicability of PHIPA*

The obligations of *PHIPA* apply when a health information custodian collects personal health information. Exploring the definitions of these terms reveals that it is likely *PHIPA* would apply to a private professional sports organization, given certain assumptions.

The collection of biometric data through wearable devices by professional sports teams easily meets the definitions given in *PHIPA* for the terms "personal health information" and to "collect." *PHIPA* defines personal health information as "identifying information about an individual in oral or recorded form, if the information relates to the physical or mental health of the individual."[68] The biometric data of athletes would easily be captured by this definition. This data is a detailed analysis of the athlete's physical health, and by its very nature would be identifying information about the specific athlete. *PHIPA* further defines collection, "in relation to personal health information, [as meaning] to gather, acquire, receive or obtain the information by any means from any source."[69]

---

[65] Ontario, Information and Privacy Commissioner, "A Guide to the *Personal Health Information Protection Act*", (Toronto: IPC, December 2004), online (pdf): <https://www.ipc.on.ca/wp-content/uploads/Resources/hguide-e.pdf>.
[66] Personal Health Information Protection Act, SO 2004, c3, s 1(a)(b).
[67] *Ibid* at s 1(c).
[68] *Ibid* at s 4(1)(a).
[69] *Ibid* at s 2.

Given this broad definition, the purposeful use of sophisticated biometric trackers would qualify under this definition as well.

Where the uncertainty as to applicability arises is whether the professional sports team or the team physician is considered a health information custodian. *PHIPA* defines a health information custodian as a "person or organization described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or the work described in the paragraph," and then goes on to list eight situations.[70]

The first situation is the most applicable, as it refers to "a health care practitioner,"[71] which is further defined to include "(a) a person who is a member within the meaning of the *Regulated Health Professions Act, 1991* and who provides health care, … or (d) any other person whose primary function is to provide health care for payment."[72] While this focus on individuals in the definition would seem to exclude the private sports organization, given the biometric data's personal nature, and the stated purpose of the act to protect this information, a purposive interpretation could capture the sports organization vicariously through the actions of the team physician administering or interpreting the biometric data collected.

Assuming that the team's physician is not a member of a health profession college, negating subsection (a) of the definition, there is still a strong argument that the team would be captured under subsection (d), as collecting biometric data would be considered providing health care. Health care is defined under *PHIPA* as:

> any observation, examination, assessment, care, service or procedure that is done for a health-related purpose and that (a) is carried out or provided to diagnose, treat or maintain an individual's physical or mental condition, (b) is carried out or provided to prevent disease or injury or to promote health…[73]

---

[70] *Ibid* at s 3(1).
[71] *Ibid* at s 3(1)(a).
[72] *Ibid* at s 2.
[73] *Ibid* at s 2.

As discussed earlier, part of the purpose of tracking biometric data is to gather more information on how athletes are recovering from injuries and to maintain their health, a purpose which would seemingly fit into the above definition. Therefore, if the team physician is directly involved in the collection and interpretation of biometric data, there is a strong argument that *PHIPA* would apply. The organization's physician provides health care for the team, and part of the purpose of collecting the athlete's biometric data is to improve their health. Even if the team physician were not sufficiently involved in the administration of the biometric tracking, the staff member responsible for its administration would likely be seen as a health care practitioner. Given the above purposive interpretation of health care, the staff member's actions in administering the biometric tracking devices would likely be captured under the above definition, making the staff member a health care practitioner, and in turn a health information custodian under *PHIPA*. Overall, there is a strong argument that a professional sports team based in Ontario that collects the biometric data of its athletes would be subject to the obligations of *PHIPA*.

Further, while conclusions as to conflicts of law are beyond the scope of this paper, the broad definitions given to the terms "individual", "health care", and "health care practitioner" raise the potential for *PHIPA* to apply to teams based outside of Ontario while they are playing (and collecting biometric data) inside of Ontario. While Provincial legislatures lack the legislative competence to enact laws having extraterritorial effect, this competence clearly exists within the boundaries of the province.[74]

### *Obligations Under PHIPA*

Similar to the CBAs discussed earlier, if *PHIPA* applies, its application results in various obligations on the team regarding the collection, storage, and use of the biometric data.

To begin, the team has to receive the athlete's consent before collecting their biometric data.[75] This consent must be knowledgeable. The athlete has to know why the biometric data is being collected and used, and know that that they have

[74] Peter Hogg, *Constitutional law of Canada*, 5th ed (Scarborough: Thomson Carswell, 2017) at s 13.3(a)-(b).
[75] *PHIPA*, *supra* note 60 at s 29.

the ability to withhold consent.[76] Further, the athlete's consent cannot be implied since the biometric data is likely shared with multiple people within the organization and the athlete must expressly consent to this data sharing.[77]

The team can only use the biometric data for the purposes that were disclosed to the athlete when it was collected, and for functions reasonably necessary to carry out the disclosed purpose.[78] Further, the athlete has a legal right of access to the data record. If, upon reviewing their record, an athlete believes that the data is inaccurate or incomplete, they have a right to request that the team correct the information.[79] However, the authority still lies with the team to determine if the record is indeed inaccurate or incomplete.[80] If an athlete believes that their team has acted contrary to the obligations under *PHIPA*, they can file a complaint with the Information and Privacy Commissioner.[81] The Information and Privacy Commissioner can then make an order compelling the team to take the actions necessary to become compliant with *PHIPA*.[82] Absent from the legislation are provisions dictating or expanding upon the ownership of the data collected.

If non-Ontario teams were found to be subject to *PHIPA* while playing in Ontario, these teams would face the additional obligation to either obtain the athlete's consent, or establish that disclosure is reasonably necessary to the provision of health care to the athlete, before the biometric data could be disclosed outside of Ontario.[83]

---

[76] *Ibid* at ss 18(1)(b), 18(5).
[77] *Ibid* at ss 18(3)(a), 50(1)(a).
[78] *Ibid* at ss 37(1)(a).
[79] *Ibid* at s 55(1).
[80] *Ibid* at s 55(9).
[81] *Ibid* at s 56(1).
[82] *Ibid* at s 61(1).
[83] *Ibid* at s 50(1).

### *Conclusions Regarding CBA Compliance with PHIPA*

The obligations set out in *PHIPA* represent the minimum that must be done by those who fall within the definition of a health information custodian. In some regards the CBAs in the NBA and MLB go above the standards set by *PHIPA*. Both agreements require teams to provide athletes with written explanations of the biometric data to be collected, and the purpose for which the team is collecting it, provisions which would satisfy the requirement for express knowledgeable consent contained in *PHIPA*. Both CBAs further give athletes explicit rights of access to the biometric data, meeting this obligation in *PHIPA* as well. While the CBAs are silent in regard to other obligations under *PHIPA*, neither of the CBAs directly contradicts *PHIPA*.

For all leagues, whether or not they meet the definition of a health information custodian, the obligations imposed by *PHIPA* should serve as an indication of best practices for the management of biometric data. These obligations address many of the potential harms associated with the collection of biometric data identified earlier by giving the athlete knowledge of the information collected and by respecting the privacy interests of the athlete. So, while *PHIPA* does not assist us in determining who has ownership over biometric data collected, the legislation is at least instructive in how the data should be handled once collected.

## Personal Information Protection and Electronic Documents Act

The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) is a piece of federal legislation that governs the collection, use and disclosure of all personal information, not just health information, by private entities.[84] While there is some uncertainty as to whether *PHIPA* applies to professional sports teams, it is clear that *PIPEDA* is applicable to Ontario based professional sports teams.

[84] *PIPEDA*, *supra* note 60 at s 3.

***Applicability of PIPEDA***

*PIPEDA* applies to organizations that collect, use, or disclose personal information in the course of commercial activities, and the biometric data collected from athletes by teams would easily fall into these defined terms.[85] To begin, the biometric data of athletes would likely be captured under the definition of personal information because it is linked to an individual.[86] As the Supreme Court of Canada has held, the definition of personal information must be given a broad and expansive interpretation.[87]

Second, a plain reading of the statute supports the collection of the biometric data as falling under the definition of a commercial activity. *PIPEDA* defines commercial activity to refer to, "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character…"[88] As the acquisition of talented athletes, and their continued and improved health and fitness, is essential to the commercial success of the team, it is very likely that the collection of athletes' biometric data by their teams would be considered in the course of a commercial activity.

This interpretation is further supported by the case law on this section. In *Rousseau v. Wyndowe*[89] the Federal Court of Appeal evaluated whether an independent medical examination undertaken to obtain disability benefits was of a commercial nature. To do so, the court broke down the relationships involved. The relationship between the doctor and the insurance company, who is paying for the independent medical examination, was of a commercial nature, and the relationship between the insured and the insurance company was clearly of a commercial nature. In the context of these two commercial relationships, the court found that the introduction of the third relationship, between the insured and the doctor, did not defeat the commercial nature of the overall transaction. This analysis can be directly applied to the situation of professional athletes who have their biometric data tracked. The relationship between the athlete and the

---

[85] *Ibid* at s 4(1)(a).
[86] *Ibid* at s 2(1).
[87] See Canada (Information Commissioner) v Canada (Commissioner of the Royal Canadian Mounted Police), 2003 SCC 8, [2003] 1 SCR 66, at para 23.
[88] *PIPEDA*, *supra* note 60 at s 2(1).
[89] 2008 FCA 39.

team is clearly commercial in nature, as is the relationship between the physician and/or technicians collecting the biometric data. As the court explained in *Rousseau*, the physician and/or technician is merely the agent of the team, and the collection of the biometric data would be an element of the commercial relationship between the team and its athletes.[90]

It should be noted, however, that *PHIPA* and *PIPEDA* are effectively mutually exclusive in their application. If a team is found to be a health information custodian under *PHIPA*, then the obligations under *PIPEDA* are prescribed not to apply.[91]

Again, while conclusions as to conflicts of law are beyond the scope of this paper, there is precedent for the obligations of *PIPEDA* to apply to non-Canadian teams while they are playing (and collecting biometric data) inside of Ontario if there exists a "real and substantial connection" between the parties and/or the facts giving rise to the complaint in Canada.[92]

### *Obligations Under PIPEDA*

As with *PHIPA*, *PIPEDA* is very instructive in setting out standards for the collection, use, and disclosure of the biometric information collected, and addresses many of the potential harms identified earlier. However, *PIPEDA* also shares *PHIPA's* issue; it does not provide any guidance as to the ownership rights over the personal information data collected. Instead it only dictates how the personal information can be collected and used. Regardless, a brief review of the obligations imposed demonstrates the further regulations with which a professional sports team must comply while collecting its athletes' biometric data.

*PIPEDA* would obligate professional sports teams to collect the biometric data of athletes in accordance with the obligations set out in Schedule 1 of the act.[93] These obligations echo many of the requirements found in *PHIPA* and negotiated into CBAs. For the team to comply with Schedule 1 of *PIPEDA*, they must get the athlete's consent before collecting their data.[94] The team must

---

[90] *Ibid* at paras. 35-36.
[91] Health Information Custodians in the Province of Ontario Exemption Order, SOR 2005, Reg 399, s 1.
[92] See T (A) v Globe24h.com, 2017 FC 114; Lawson v Accusearch Inc, 2007 FC 125.
[93] *PIPEDA*, *supra* note 60 at s 5(1).
[94] *Ibid* at Schedule 1, 4.3.

disclose to the athlete how the data will be used before it is collected, can only collect data that is necessary for this purpose, and can only use the data for this stated purpose.[95] If the team wants to use the data for a new purpose, they must get the athlete's consent beforehand.[96] The athlete has a right to access their biometric data, and can challenge inaccurate or incomplete data.[97] Similar to the MLB's CBA, the team also has the obligation to ensure that the biometric data collected is stored securely.[98] Further, the team must identify an individual responsible for compliance with these obligations, and to whom the athletes would bring forward any concerns with compliance.[99]

Unlike privacy laws established by the European Union that prohibit the transfer of personal information to another jurisdiction without adequate protection, *PIPEDA* places the obligation for compliance with the organization. Thus, if *PIPEDA* is found to apply to the biometric data collected by a non-Canadian team playing inside of Ontario, the team would not need to demonstrate that the privacy protections in the United States of America were adequate. Rather, the team would be held directly accountable for the protection of the personal information.[100]

## ANALGOUS CASE LAW

The CBAs and the legislation all give detailed regulations for the collection, use, and disclosure of biometric data, yet were all silent on the question of ownership. As such, case law should be considered to determine whether the athlete or the team owns the biometric data. While this question has not been directly tested in court, we can look to the analogous situation of patient medical records for an answer.

---

[95] *Ibid* at Schedule 1, 4.2; Schedule 1, 4.4; Schedule 1, 4.5.
[96] *Ibid* at Schedule 1, 4.2.4.
[97] *Ibid* at Schedule 1, 4.9; Schedule 1, 4.9.5.
[98] *Ibid* at Schedule 1, 4.7.1.
[99] *Ibid* at Schedule 1, 4.10.
[100] Office of the Privacy Commissioner of Canada, "Guidelines for Processing Personal Data Across Borders" (January 2009) online: <https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/>.

Ownership of patient medical records presents a strong analogy to the ownership of biometric data due to the nature of the information in question. In both situations, the information is of a fundamentally intimate and personal nature to the data's source, yet the individual is unable to collect the information without utilizing the skill and knowledge of others. This similarity can be demonstrated through the comparison of a physician who runs a test, interprets the results, and writes down her medical opinion into the patient's medical record to the team manager who measures an athlete's biometric performance during a practice, and uses the software and their knowledge to evaluate the athlete. The functions of both a physician and team manager in these examples are fundamentally similar, and often times would be taking the same measurements. Therefore, evaluating discussions over the ownership of patient's medical records will provide informative and influential insight into the questions of ownership over the biometric data of professional athletes.

The Supreme Court of Canada tackled this exact question in the 1992 case of *McInerney v MacDonald*.[101] Various physicians had treated the patient, Mrs. MacDonald, and her medical record contained notes and reports from each of these physicians over the years. When Mrs. MacDonald began seeing Dr. McInerney, Dr. McInerney advised Mrs. MacDonald to stop the medication that had been prescribed by previous physicians. Naturally, the nature of this advice made Mrs. MacDonald begin to question the competency of her previous physicians. As a result, Mrs. MacDonald wrote to Dr. McInerney to request a copy of her complete medical record. Dr. McInerney replied by sending only copies of the information she had prepared herself but refused to send copies of any material prepared by other physicians. She claimed that work was the property of the other respective doctors and that Mrs. MacDonald would have to contact the other physicians individually to gain access to these records.[102] In turn, Mrs. MacDonald then made an application to the New Brunswick Court of Queen's Bench for an order directing the disclosure of her full medical record.[103] Reflecting the difficult nature of answering this question, each level of court relied

[101] [1992] 2 SCR 138, [1992] SCJ No 57 [*McInerney SC*].
[102] *Ibid,* at para 2.
[103] *Ibid,* at para 3.

on different legal principles in coming to their answer regarding the questions of ownership and access.

At the trial level, the court looked to the relationship between solicitor and client, opining that "[ownership] of documents prepared by a lawyer on behalf of a client rests with the client in a solicitor-client relationship and with the patient in a physician-patient relationship."[104] While the Justices at the Court of Appeal split on their decision, they were united in their rejection of the trial court's reasoning. The majority found that the case did not raise an issue over ownership over the medical records, but rather over the right to access the records, and thus did not dedicate much analysis to the discussion of ownership.[105] The dissenting Justice took the time to address the trial level decision further, stating "[even] in a solicitor-client relationship, a client does not enjoy a right to the notes made by a solicitor for the benefit of the solicitor in rendering the services for a client. The Court has ruled in several decisions that the solicitor is the owner of them and need not transmit them to the client," distinguishing between documents prepared for the benefit of the client and those prepared by the solicitor to assist in the creation of client documents.[106] When applied to the analogy of biometric data collected from athletes, this distinction raises many questions about the nature of the biometric data. Would the athlete own the raw data, and the team own the report created after the data is analyzed by software? Is the client in this analogy actually the team, with the solicitor being the company who designed the biometric trackers and software? Unfortunately, the Supreme Court of Canada did not incorporate this line of reasoning, rendering this distinction of little assistance to my question.

Instead, the Supreme Court of Canada identified two issues on the appeal: who held the property rights to patient medical records, and whether a patient has a right to access their entire medical record if they do not hold the property rights to it.[107] The Court wasted little ink on the first issue, deferring to the policy statement of the Canadian Medical Association and concluding "the physician,

---

[104] *McInerney v MacDonald*, [1990] AN-B No 106, at para 6, [1990] NBJ No 106 (CA).
[105] *Ibid* at para 27.
[106] *Ibid* at para 7.
[107] *McInerney SC, supra* note 97 at para 12.

institution or clinic compiling the medical records owns the physical record."[108] Therefore, to complete the analogy, if the institution compiling the medical record of a patient owns the physical record, then the institution compiling the biometric data of an athlete would own the biometric data. While this analogy would also give the athlete a strong right to access the biometric data, the analogy is unnecessary for this purpose as the right to access is already strongly entrenched in both collective agreements and legislation.

## CONCLUSION

After reviewing the CBAs negotiated between the players unions and the various leagues and the applicable provincial and federal legislation, the most definitive answer to the question of ownership over an athlete's biometric data is provided by the analogous case law governing the ownership of patient medical records. The party that compiles the information owns the information. Since the team owns the biometric trackers and compiles the information, the team ultimately owns the data. This conclusion raises certain ethical questions. The encroachment of these biometric tracking technologies allows for more of the professional athlete's body to be considered the property of the team, an issue that will only grow the more invasive these biometric trackers become and the more their use off the field is normalized.[109] As we have discovered, however, athletes are aware of the potential for the collection of biometric data to result in either inequitable outcomes, or the loss of privacy interests, and they have made their concerns known in the most recently negotiated CBAs. As discussed earlier, provisions in the CBAs for the NBA and MLB explicitly prevent the biometric data from being used to influence contract negotiations, from either party monetizing the data, and put in place procedures for the approval and use of the monitoring devices. With CBA renegotiations quickly approaching for the other leagues, the rights and regulations found in the CBAs for the NBA and MLB will almost certainly influence these future negotiations. As this paper has demonstrated, representatives from these unions should make the regulation and

[108] *Ibid* at 14.
[109] Venook, *supra* note 14.

protection of athletes' biometric data a priority. The failure to do so could have significant detrimental impacts on professional athletes.