Athlete Biometric Data in Soccer: Athlete Protection or Athlete Exploitation?

Adam Garlewicz

Follow this and additional works at: https://via.library.depaul.edu/jslcp

Part of the Entertainment, Arts, and Sports Law Commons

Recommended Citation
Available at: https://via.library.depaul.edu/jslcp/vol16/iss1/2

This Article is brought to you for free and open access by the College of Law at Via Sapientiae. It has been accepted for inclusion in DePaul Journal of Sports Law by an authorized editor of Via Sapientiae. For more information, please contact digitalservices@depaul.edu.
Athlete Biometric Data in Soccer: Athlete Protection or Athlete Exploitation?

Cover Page Footnote
Adam Garlewicz, J.D. Candidate, DePaul University College of Law, 2020; B.A. Journalism and Public Relations & Advertising, DePaul University, 2017. I would like to thank Julie Garabedian, Ryan Probasco, and Lisa Grzelak for their feedback throughout my writing process. I would also like to thank my family for their constant support.
1. INTRODUCTION

The next kick, one right-footed strike of a soccer ball twelve yards from the goal, will change the world forever. This next kick will transform lives, alter economies, and turn an individual into a hero, cementing them a permanent place in history. With the result of this next kick, an entire country will either bask in euphoric glory or grieve with insuppressible sorrow. Uncontrollable tears will flow regardless. This next kick can only have three outcomes: the ball will go in the goal; the goalie will save the shot; or the player will miss.

It’s time for the kick. The referee hands the ball to the player. The player, with a heart racing faster than ever before, places the ball on the penalty spot. The player beams with confidence and looks ready for the moment, but in reality, the player feels as if he/she are about to crumble from the pressure. The player’s coach chose this player for this specific moment. The coach’s reason behind the decision may vary, but this player was chosen either because they are the team’s deadliest striker or their most composed player. For years, throughout the qualification process and the tournament itself, the coach knows this player far more than someone outside the team can imagine. Not only does the coach know the player’s physical traits on the soccer pitch, but the coach understands the player’s stamina because of various devices tracking their heart rate and average distances run during games. From wearable technologies that the player wears during training or games, the coach is also able to assess the player’s fitness and determine if he/she is suffering from any nagging and/or reoccurring injuries.

On the other side of the ball, the goalie stands tall and stretches out his/her arms, shifting from side-to-side to disorient the player. The goalie knows that he/she is not expected to save the shot from such close range, but he/she is convinced he/she will. In the player’s mind, he/she is just as ready for this moment as the offensive player. The goalie has spent countless hours studying the body movements of the player, hoping to anticipate where the player will kick. The goalie has statistics of the player’s attempts from the penalty spot and film on the player’s certain habits. In addition, it is likely that the goalie has similar information to that of the coach on the player’s stamina, fitness, and health, and vice versa.

The referee blows the whistle. The fans in the sold-out stadium, who were rowdy throughout the game, are all on their feet, but not a sound can be heard. An eerie silence fills the stadium. The player takes a deep breath and steps towards the soccer ball. The player plants his/her left foot about six inches behind and to the left of the ball, and with all of his/her might, heart, and strength, kicks the ball with his/her right foot. One dream is fulfilled, while another is shattered.

This portrayal hypothetically describes a World Cup Final game that progresses into a penalty shootout. Every player, from amateur to professional, dreams of this chance to win the World Cup for his/her country by either converting or saving a penalty kick; however, this illustration is especially useful because it touches on the main ideas this article will address. All of the human medical information that was used by the player, goalie, and coach to create a strategy for this life-altering penalty kick can be referred to as Athlete Biometric Data (“ABD”).
ABD is comprised of three words; athlete, biometric, and data. “Athlete” refers to the player, “biometric” refers to any metric related to human features,1 and “data” is objective information, such as measurements or statistics, used as a basis for reasoning, discussion, or calculation.2 Biometric data is the unique and permanent biometric information collectable and/or measurable from an individual.3 Examples of collectible biometric data include fingerprints, facial and voice features, iris patterns, hand geometry, and behavioral characteristics.4 A recent article from the American Bar Association stated the following on biometrics: “Biometrics measure and analyze people’s unique physical and behavioral characteristics. Biometrics’ many uses include identification, access controls, testing, and numerous other rapidly evolving business applications.”5

It is not as easy to define ABD. Kristy Gale, author of a two-part series analyzing the legal implications in the collection of ABD, points out that “[a] precise definition [of ABD] is difficult to craft because of the many ways in which ABD interacts with the sports industry.”6 Gale suggests that to understand ABD, it is important to “look to definitions used (1) in the field of biometrics, (2) in common parlance by those in the sports industry, (3) under governing law and by the courts, and (4) in contractual language.”7 These four areas will be referenced throughout this article.

There are numerous legal issues surrounding the collection of ABD, and new issues are continuously raised because of the advancements in technology related to the collection of ABD. This article will focus on a few of the present legal issues dealing with ABD related to consent, privacy, publicity, and contract disputes. There will be a brief discussion of ABD and how it is used in fantasy sports and videogames. In order to fully understand issues dealing with ABD, this article will begin with a legal discussion regarding the collection of biometric data and what it means to possess an individual’s biometric data. In addition to learning about the various state and federal statutes across the United States that address biometric data, it is essential to understand how courts are applying these statutes. Soccer is a global sport, but part one of this article will discuss law in the United States.

---

3 Porter, supra note 1.
4 Id.
7 Id.
II. LAW GOVERNING THE COLLECTION OF BIOMETRIC DATA IN THE UNITED STATES

A. Statutes

Currently, four states (Illinois, Texas, Washington, and California) have statutes regarding the collection of biometric data, and there is proposed legislation in other states.\(^8\) There are other jurisdictions that have enacted biometric information privacy acts,\(^9\) but this article will cite the statutes in the four aforementioned states. To date, the most influential and controversial statute dealing with the collection of biometric data is the Biometric Information Privacy Act ("BIPA"), enacted in Illinois in 2008. The most recent legislation is the California Consumer Privacy Act, which went into effect January 1, 2020.\(^10\) It gives California residents certain rights to control what information companies collect on them and how that information is used.\(^11\) This article focuses on "biometric data," so it is important to look at how these statutes define similar terms. Under BIPA, biometric information is defined as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."\(^12\) The following chart shows how "biometric identifier" is defined in Illinois, Texas, and Washington, and how "biometric information" is defined in California.

<table>
<thead>
<tr>
<th>State</th>
<th>Definition of “biometric identifier”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illinois</td>
<td>“a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.”(^14)</td>
</tr>
<tr>
<td>Texas</td>
<td>“a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.”(^15)</td>
</tr>
<tr>
<td>Washington</td>
<td>“data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual.”(^16)</td>
</tr>
</tbody>
</table>

---

14 Id.
“an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.”¹⁷

Even though there are countless terms associated with biometrics such as “biometric data,” “biometric information,” and “biometric identifiers,” it is important to remember that all would be considered one in the same for ABD and all represent unique characteristics related to specific individuals. The next important legislative factor to consider is how these statutes address consent, notice, and/or disclosure requirements when an individual’s biometric data is collected. Defining consent is critical because if an individual gives the required permission for his/her biometric data to be collected, there should not be a violation. Furthermore, describing the disclosure or notice requirements for collecting biometric data is vital because companies need to be aware of the potential consequences associated with a violation. The following chart shows how the states mentioned above attempt to address the consent, notice, and/or disclosure issues.

<table>
<thead>
<tr>
<th>State</th>
<th>Consent/Notice/Disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illinois</td>
<td>“No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:</td>
</tr>
<tr>
<td></td>
<td>(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;</td>
</tr>
<tr>
<td></td>
<td>(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected or stored;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State</th>
<th>Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>Texas</td>
<td>“[a] person may not capture a biometric identifier of an individual for a commercial purpose unless the person: (1) informs the individual before capturing the biometric identifier; and (2) receives the individual's consent to capture the biometric identifier.”</td>
</tr>
<tr>
<td>Washington</td>
<td>“[n]otice is a disclosure, that is not considered affirmative consent, that is given through a procedure reasonably designed to be readily available to affected individuals. The exact notice and type of consent required to achieve compliance with subsection (1) of this section is context-dependent.”</td>
</tr>
<tr>
<td>California</td>
<td>A business that collects a consumer’s personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.”</td>
</tr>
</tbody>
</table>

A major difference between BIPA and the other statutes is that BIPA requires notice and consent for the collection of a biometric identifier, regardless of the purpose of collection. In contrast, the other statutes require notice and consent only if the collection of a person’s biometric identifiers is used for a commercial purpose. Employer punch-in clocks that scan an employee’s fingerprint for timekeeping purposes illustrate this important difference. Here, the collection of an individual’s biometric identifier is not being used for commercial purposes. Illinois requires consent, while other states typically do not. If the Illinois employer does not

---

22 McGinley, supra note 8.
23 Id.
obtain the employee’s consent, the employer is violating BIPA and is subject to fines as well as monetary damages.

The statutes differ on whether a private individual can sue for a violation. BIPA does provide a private individual with a right of action, stating “[a]ny person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party.” Unlike BIPA, the Washington statute only allows the attorney general of Washington to enforce the act. However, each of these statutes does provide what type of penalties can be enforced for violating the statute, with some harsher than others. The following list shows the potential liability private parties will faced after violating these statutes.

<table>
<thead>
<tr>
<th>State</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illinois</td>
<td>“A prevailing party may recover for each violation:</td>
</tr>
<tr>
<td></td>
<td>(1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;</td>
</tr>
<tr>
<td></td>
<td>(2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;</td>
</tr>
<tr>
<td></td>
<td>(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and</td>
</tr>
<tr>
<td></td>
<td>(4) other relief, including an injunction, as the State or federal court may deem appropriate.”</td>
</tr>
<tr>
<td>Texas</td>
<td>“a civil penalty of not more than $25,000 for each violation. The attorney general may bring an action to recover the civil penalty.”</td>
</tr>
<tr>
<td>Washington</td>
<td>“(1) The legislature finds that the practices covered by this chapter are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. A violation of this chapter is not reasonable in relation to the development and preservation of business and is an unfair or</td>
</tr>
</tbody>
</table>

---

BIPA contains more severe penalties than the other statutes. BIPA gives an individual a right to a private cause of action, thereby creating a larger risk and threat to companies collecting biometric identifiers in Illinois. While all four of the referenced statutes are intended to protect consumers, Washington’s statute is more of a regulation, where BIPA encourages litigation if a company is collecting biometric identifiers without consent.

The Illinois legislature originally enacted BIPA in response to the finding that the use of biometric information was growing, specifically in financial transactions. Since the enactment of BIPA in 2008, technology relating to the collection of biometric information has greatly evolved. The legislative intent of BIPA demonstrates that Illinois legislators were already

---

concerned in 2008 with the risks related to the collection of an individual’s biological information.\textsuperscript{31} The legislature stated the following:

“Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.”\textsuperscript{32}

In describing the purpose of BIPA, the legislature stated, “[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.”\textsuperscript{33} BIPA shows that Illinois is trying to get ahead of the evolving technology, and put safeguards in place for the public’s welfare. In relation to ABD, this article will address how soccer leagues and organizers do not have the same safeguards in place. These types of safeguards are important because soccer athletes should be aware that their ABD is being collected. These safeguards also deter teams and third parties from taking advantage of a soccer athlete’s ABD. The next section will address case law related to the collection and possession of biometric data.

\textbf{B. Case Law}

Legislators at the state and federal levels are starting to focus on the regulation of the collection and possession of biometric data. Courts are beginning to interpret the recent statutes, setting new precedent each year in the process. Technology used for collecting biometric data is also developing, and, therefore, there is a lack of case law available. As a result, case law dealing with the collection of biometric data in the United States is growing rapidly. The cases mentioned in the next section are beginning to shape the legal landscape of the collection of biometric data.

\textbf{1. State Cases}

Illinois is a great place to begin for an introduction on recent case law related to the collection and possession of biometric data. This is no surprise because of the magnitude of BIPA. In the last few years, Illinois has experienced a drastic rise in litigation related to the collection of biometric information and privacy.\textsuperscript{34} The seminal case in Illinois, decided by the Illinois Supreme Court in 2019, is \textit{Rosenbach v. Six Flags Entm't Corp}.\textsuperscript{35} Referring to BIPA, the court in \textit{Rosenbach} held that “an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an ‘aggrieved’ person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act.”\textsuperscript{36} \textit{Rosenbach} is especially important because of its recency, jurisdiction, and effect on jurisdictions across the United States.

\begin{itemize}
  \item \textsuperscript{31} 740 Ill. Comp. Stat. Ann. 14/5.
  \item \textsuperscript{32} \textit{Id}. 14/5(c).
  \item \textsuperscript{33} \textit{Id}. at 14/5(g).
  \item \textsuperscript{34} Charles N. Insler, \textit{Understanding the Biometric Information Privacy Act Litigation Explosion}, 106 Ill. B.J. 34, 35 (2018).
  \item \textsuperscript{35} \textit{Rosenbach v. Six Flags Entm't Corp.}, 2019 IL 123186, 129 N.E.3d 1197.
  \item \textsuperscript{36} \textit{Id}. at ¶ 40.
\end{itemize}
In *Rosenbach*, the relevant facts involved Six Flags Great America (“Six Flags”), an amusement park, using fingerprint scanners when season pass holders were entering the park.\(^{37}\) The plaintiff was the mother of a 14-year-old who had a season pass to the park.\(^{38}\) She brought suit, acting in her capacity as mother, when she learned that the park collected and stored her son’s fingerprint information, a biometric identifier, with neither her son’s nor her consent.\(^{39}\) Her son, named Alexander, had just come home from a school field trip that went to Six Flags Great America.\(^{40}\) The plaintiff asked her son for the paperwork associated with his season pass.\(^{41}\) Alexander reported that there was no paperwork and that it was all done by fingerprint scanning.\(^{42}\) Upon hearing this, the plaintiff proceeded to take action and file a complaint.\(^{43}\)

The issue in the case was “whether one qualifies as an ‘aggrieved’ person and may seek liquidated damages and injunctive relief pursuant to the Act if he or she has not alleged some actual injury or adverse effect, beyond violation of his or her rights under the statute.”\(^{44}\) Under BIPA, any aggrieved person by a violation of the Act’s provisions may recover from the offending party for each violation, among others, actual damages and reasonable attorney’s fees.\(^{45}\)

Six Flags never disclosed Alexander’s personal biometric information to a third party. Therefore, the defendants argued, among other things, that the plaintiff lacked standing to sue because the plaintiff had suffered no actual injury or threatened injury.\(^{46}\) The plaintiff’s complaint contained three counts.\(^{47}\) Count I claimed that the defendants violated section 15(b) of the Act by:

“(1) collecting, capturing, storing, or obtaining biometric identifiers and biometric information from Alexander and other members of the proposed class without informing them or their legally authorized representatives in writing that the information was being collected or stored; (2) not informing them in writing of the specific purposes for which defendants were collecting the information or for how long they would keep and use it; and (3) not obtaining a written release executed by Alexander, his mother, or members of the class before collecting the information.”\(^{48}\)

Count II requested injunctive relief under the Act to compel defendants to make disclosures pursuant to the Act's requirements and to prohibit them from violating the Act going forward,\(^{49}\) and count III asserted a common-law action for unjust enrichment.\(^{50}\) At the circuit

\(^{37}\) *Id.* at ¶ 4.

\(^{38}\) *Id.* at ¶ 5.

\(^{39}\) *Id.* at ¶ 10.

\(^{40}\) *Id.* at ¶ 5.

\(^{41}\) *Id.*

\(^{42}\) *Id.* at ¶ 7.

\(^{43}\) *Id.* at ¶ 10.

\(^{44}\) *Id.* at ¶ 1.


\(^{46}\) *Rosenbach*, 129 N.E.3d at ¶ 12.

\(^{47}\) *Id.* at ¶ 11.

\(^{48}\) *Id.*

\(^{49}\) *Id.*

\(^{50}\) *Id.*
court level, Illinois’ trial court, the defendants filed a motion to dismiss all three counts.\footnote{Id. at ¶ 12.} The circuit court denied the motion as to counts I and II, but granted the motion as to count III.\footnote{Id. at ¶ 13.} Defendants sought interlocutory review\footnote{“An interlocutory appeal, or interlocutory review, is an appeal that is made by the parties to a case while a trial in the matter is still ongoing. An interlocutory appeal asks an appellate court to review a decision made by the trial court.” Legal Dictionary, Definition of Interlocutory, (Oct. 12, 2018), https://legaldictionary.net/interlocutory/ (last visited May 5, 2020).} of the circuit court’s ruling.\footnote{Rosenbach, 129 N.E.3d at ¶ 14.} Two questions of law were identified by the circuit court:

(1) “[w]hether an individual is an aggrieved person under § 20 of the Illinois Biometric Information Privacy Act, 740 ILCS 14/20, and may seek statutory liquidated damages authorized under § 20(l) of the Act when the only injury he alleges is a violation of § 15(b) of the Act by a private entity who collected his biometric identifiers and/or biometric information without providing him the required disclosures and obtaining his written consent as required by § 15(b) of the Act,” and

(2) “[w]hether an individual is an aggrieved person under § 20 of the Illinois Biometric Information Privacy Act, 740 ILCS 14/20, and may seek injunctive relief authorized under § 20(4) of the Act, when the only injury he alleges is a violation of § 15(b) of the Act by a private entity who collected his biometric identifiers and/or biometric information without providing him the required disclosures and obtaining his written consent as required by § 15(b) of the Act.”\footnote{Id.}

The Illinois Appellate Court for the Second Circuit answered both questions in the negative.\footnote{Id. at ¶ 15.} In the appellate court’s view:

“a plaintiff is not ‘aggrieved’ within the meaning of the Act and may not pursue either damages or injunctive relief under the Act based solely on a defendant's violation of the statute. Additional injury or adverse effect must be alleged. The injury or adverse effect need not be pecuniary, the appellate court held, but it must be more than a “technical violation of the Act.”\footnote{Id.}

The Illinois Supreme Court granted plaintiff’s petition for appeal.\footnote{Id. at ¶ 16.} A large portion of the Illinois Supreme Court’s opinion discussed BIPA. The Court explained the Act “was enacted in 2008 to help regulate the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.”\footnote{Id. at ¶ 19.} Defendants argued that the Illinois legislature intended to limit a plaintiff’s right to bring a cause of action under the Act to circumstances where he or she sustained some sort of actual damage, “beyond violation of the rights conferred by the statute, as the result of the defendant’s conduct.”\footnote{Id. at ¶ 25.} The Court responded
to defendant’s argument by stating “This construction is untenable. When the General Assembly has wanted to impose such a requirement in other situations, it has made that intention clear.” 61

The Court went on to provide examples of acts where actual damage must be alleged by the plaintiff in order to bring an action, like the Illinois Consumer Fraud and Deceptive Business Practices Act.62

In concluding that plaintiff was “aggrieved” under BIPA, the Illinois Supreme Court referenced an Illinois case from more than a century ago, Glos v. People.63 The Court quoted Glos, which stated that “[a] person is prejudiced or aggrieved, in the legal sense, when a legal right is invaded by the act complained of or his pecuniary interest is directly affected by the decree or judgment.”64

The court further stated that “[t]his understanding of the term [aggrieved] has been repeated frequently by Illinois courts and was embedded in our jurisprudence when the Act was adopted.”65 Additionally, in concluding that the plaintiff sufficiently pled a cause of action under the Act, the court reasoned:

“[W]hen a private entity fails to comply with one of section 15’s requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach… [S]uch a person or customer would clearly be “aggrieved” within the meaning of section 20 of the Act and entitled to seek recovery under that provision. No additional consequences need be pleaded or proved. The violation, in itself, is sufficient to support the individual's or customer's statutory cause of action.”66

In sum, the Illinois Supreme Court held that a plaintiff need not suffer an actual injury to be an “aggrieved” person under the Act.67 The plaintiff was entitled to relief even without alleging “actual injury or damage beyond infringement of the rights afforded them under the law.”68 The Court stated:

“Contrary to the appellate court's view, an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an “aggrieved” person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act. The judgment of the appellate court is therefore reversed, and the cause is remanded to the circuit court for further proceedings.”69

61 Id.
62 Id.
63 Id. at ¶ 30.
64 Id. (quoting Glos v. People, 259 Ill. 332, 340, 102 N.E. 763 (1913)).
65 Id. at ¶ 31.
66 Id. at ¶ 33.
67 Id. at ¶ 40.
68 Id. at ¶ 38.
69 Id. at ¶ 40.
Presently, *Rosenbach* is the most influential case regarding biometric data privacy in Illinois and has completely changed the landscape in terms of litigating under BIPA. *Rosenbach* is important to this article because *Rosenbach* shows how athletes may have standing when it comes to illegal collection or possession of their ABD. In addition, *Rosenbach* has a role in predicting how courts will interpret statutes similar to BIPA in the near future. The following case is an example.

In *Rottner v. Palm Beach Tan, Inc.*,70 an Illinois Appellate Court reversed an Illinois Circuit Court’s decision because of *Rosenbach*.71 In comparing the plaintiff in *Rosenbach* to the plaintiff in *Rottner*, the court held that the plaintiff had “standing to sue and has adequately stated a claim for liquidated damages under section 20 of the Act, even if she has alleged only a violation of the Act and not any actual damages beyond violation of law.”72 In *Rottner*, the plaintiff sued Palm Beach Tan, a tanning salon, because the salon required her fingerprint each time she sought to use the tanning services.73 The parallels between *Rosenbach* and *Rottner* are obvious, especially with both Six Flags and Palm Beach Tan using fingerprints as a form of access to services provided by each company. The plaintiff claimed an award of liquidated damages under section 20 of the Act.74 Section 20 provides that “A prevailing party may recover for each violation… against a private entity that negligently violates a provision of this Act, liquidated damages of $ 1,000 or actual damages, whichever is greater.”75 The court in *Rottner* applied the holding in *Rosenbach*, and held that “[a] plaintiff who proves a violation of the Biometric Information Privacy Act may recover liquidated damages without proof of actual damages beyond the violation of the Act.”76 Although there are several other Illinois cases that cite to *Rosenbach*, it is important to briefly discuss a few relevant federal cases.

2. Federal Cases

In *Namuwonge v. Kronos, Inc.*,77 a case from the Northern District of Illinois, the court cited *Rosenbach* when addressing the issue of whether a company was in possession of someone’s biometric information.78 In *Namuwonge*, the plaintiff’s employer used a time-keeping system that required employees to scan their fingerprint as a means of authenticating and monitoring time worked.79 Kronos, a leading provider in workforce management software and services, supplied the timekeeping system to plaintiff’s employer.80 Plaintiff alleged that Kronos failed to provide to plaintiff and her fellow employees “with a written, publicly available policy explaining their retention schedules and guidelines for permanently destroying biometric data in their possession.”81 Plaintiff further alleged that because Kronos did not disclose the purposes for their collection and use of biometric data, the employees had no idea whether Kronos “sells,
discloses, re-discloses, or otherwise disseminates their biometric data.” Kronos’ argued that they did not possess plaintiff’s biometric information because possession required the exercise of dominion and control over the biometric data to the exclusion of others.

“Applying the lessons of Rosenbach,” the court first looked to the statutory of language of BIPA to determine if Kronos was in possession of plaintiff’s biometric information. The court in Namuwonge concluded that Kronos was in possession of plaintiff’s biometric information, because, even though the Act does not define possession, there is “no indication that the ordinary meaning of possession does not apply.” The court stated plaintiff’s allegation that her employer “disclosed their employees’ fingerprint data to Kronos sufficiently alleges that Kronos possessed the fingerprint data collected by [employer].” In Namuwonge, the court also concluded that because “Kronos did not publish a data-retention policy and it is unclear… when any retention policy was formulated relative to when Kronos possessed the [] employees’ biometric information, the Court finds the allegations plausible to state a claim.”

As it relates to the subject matter of this article, cases like Namuwonge demonstrate how third parties can be liable for possessing an individual’s ABD without their consent. As this article will later discuss, teams (employers) use the athlete’s ABD, but third parties (i.e., manufacturers of wearable technologies that collect ABD) may possess the athlete’s ABD and try to financially exploit that data. Namuwonge also shows how courts are defining “possession” of biometric data. In Rosenbach, the court explained that the plaintiff does not to have suffered from an “actual injury” to have state a claim for a violation of the Act. Following Namuwonge, data collection companies have to be aware that whenever someone discloses a third party’s biometric data to them, they are considered to be in “possession” of that biometric data under the Act, regardless of what happens with the data. As a result, companies have to make sure that they have adequate data-retention and disclosure policies in place to avoid liability under BIPA.

In addition to its influence in Illinois, Rosenbach is beginning to have an effect on jurisdictions across the country. For example, in Patel v. Facebook, Inc., the Ninth Circuit upheld that plaintiffs do not need to allege a concrete injury-in-fact for purposes of Article III standing under BIPA. The court held that “[b]ecause a violation of the Illinois statute injures an individual's concrete right to privacy, we reject Facebook’s claim that the plaintiffs have failed to allege a concrete injury-in-fact for purposes of Article III standing.”

In Patel, a class action lawsuit, the plaintiffs alleged that Facebook subjected them to facial-recognition technology without complying with BIPA. Plaintiffs filed their complaint in the Northern District of California, which had jurisdiction because one of Facebook’s six data

82 Id.
83 Id. at 283.
84 Id.
85 Id. at 284.
86 Id.
87 Id.
89 Id. at 1267.
90 Id.
91 Id.
centers are located in California.\textsuperscript{92} These data centers contain the servers in which the face template data is stored.\textsuperscript{93} The Facebook technology subject to the complaint involved Facebook technology that “extracts the various geometric data points that make a face unique, such as the distance between the eyes, nose, and ears, to create a face signature or map.”\textsuperscript{94} This is an example of a “biometric identifier” under BIPA. After collecting the facial data, Facebook then compares the face signatures to other faces in their database of user face templates.\textsuperscript{95}!!

Using similar arguments made by Six Flags in \textit{Rosenbach}, Facebook argued that the “complaint describes a bare procedural violation of BIPA rather than injury to a concrete interest, and therefore plaintiffs failed to allege that they suffered an injury-in-fact that is sufficiently concrete for purposes of standing.”\textsuperscript{96} After citing to \textit{Rosenbach}, the court concluded that the plaintiffs had standing.\textsuperscript{97} The court stated, “[b]ecause we conclude that BIPA protects the plaintiffs’ concrete privacy interests and violations of the procedures in BIPA actually harm or pose a material risk of harm to those privacy interests, the plaintiffs have alleged a concrete and particularized harm, sufficient to confer Article III standing.”\textsuperscript{98} The court also held that “the district court did not abuse its discretion in certifying the class.”\textsuperscript{99}

\textit{Patel} is important to the legal landscape of biometric data collection, not only because it shows that other jurisdictions will apply \textit{Rosenbach} and BIPA, but also because it shows that federal courts will grant class action certification.\textsuperscript{100} In states like California, where technology giants like Facebook have data collection centers, \textit{Patel} illustrates that plaintiffs from Illinois will be able to have standing and litigate their cases in these states. The courts will apply BIPA under \textit{Rosenbach}’s interpretation. Further, \textit{Patel} shows that courts will grant conditional class certification and not be afraid to grant large statutory damages. This can be very costly to large technology companies that do not obtain consent for biometric data collection. Finally, it is important to note that \textit{Patel} discusses privacy interests and uncovers the harm that can be caused to those privacy interests by mass collection and storage of users’ biometric data. Potential harm to privacy interests is one of the most common issues relating to the collection of a soccer athlete’s ABD.

The following chart summarizes the holdings of other federal cases related to the collection and/or privacy of biometric data.

<table>
<thead>
<tr>
<th>Case Citation</th>
<th>Holding</th>
</tr>
</thead>
<tbody>
<tr>
<td>\textit{Rogers v. CSX Intermodal Terminals, Inc.}, 409 F. Supp. 3d 612 (N.D. Ill. 2019).</td>
<td>Truck driver was an “aggrieved person” under BIPA and stated adequate claim for violation of BIPA against rail terminal operator, where operator collected his biometric information</td>
</tr>
</tbody>
</table>

\textsuperscript{92} Id. at 1268.
\textsuperscript{93} Id.
\textsuperscript{94} Id.
\textsuperscript{95} Id.
\textsuperscript{96} Id. at 1271.
\textsuperscript{97} Id. at 1274.
\textsuperscript{98} (internal citations omitted) Id. at 1275.
\textsuperscript{99} Id. at 1267.
\textsuperscript{100} This allows a large group of plaintiffs to file a lawsuit all at once, rather than filing individually. \textit{See generally} Fed. R. Civ. P. 23.
without obtaining a written release or providing him written disclosure of the purpose and duration for which his information was collected.

<table>
<thead>
<tr>
<th><strong>Rivera v. Google Inc.</strong>, 238 F. Supp. 3d 1088 (N.D. Ill. 2017).</th>
<th>The court held that plaintiffs sufficiently alleged that face templates of their features were “biometric identifiers” within meaning of BIPA where plaintiffs were the subject of photographs taken by smartphones and the images were automatically uploaded, without their consent, to a cloud-based service that scanned facial features to create face templates.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Campbell v. Facebook, Inc.</strong>, 951 F.3d 1106 (9th Cir. 2020).</td>
<td>Affirmed settlement against Facebook where “Facebook routinely captured, read, and used for several purposes the website links included in users’ private messages without their consent, and that these practices violated federal and California privacy laws.”¹⁰¹</td>
</tr>
<tr>
<td><strong>Santana v. Take-Two Interactive Software, Inc.</strong>, 717 F. App'x 12 (2d Cir. 2017).¹⁰²</td>
<td>Court held there the plaintiffs, consumers who brought a putative class action, did not have standing against the defendant, a software company that collected biometric data for use in its video games, under BIPA.</td>
</tr>
<tr>
<td><strong>Heard v. Becton, Dickinson &amp; Co.</strong>, No. 19 C 4158, 2020 WL 887460 (N.D. Ill. Feb. 24, 2020).</td>
<td>In a case where the plaintiff, a respiratory therapist, had to scan his fingerprint to access an automated medication dispensing system manufactured by the defendant, the court held that the plaintiff did not adequately plead “possession” because the plaintiff failed to allege that the defendant exercised any dominion or control over the defendant’s biometric data.</td>
</tr>
</tbody>
</table>

As a result of the recency of the cases listed above, it is important to pay close attention to case law across U.S. jurisdictions on both state and federal levels. This area of law is constantly evolving. To date, the United States Supreme Court has not addressed *Rosenbach’s* interpretation of BIPA. However, defendant Facebook, in *Patel*, did attempt to appeal the Ninth Circuit’s decision to the Supreme Court, but the petition for writ of certiorari was denied.¹⁰³ Still,

---

¹⁰¹ **Campbell v. Facebook, Inc.**, 951 F.3d 1106, 1111 (9th Cir. 2020).
the “standing issue” may in fact be argued in front of the Supreme Court one day. Nevertheless, companies within the United States need to be aware of how courts are interpreting statutory provisions related to the collection of biometric data.

III. SOCCER – THE WORLD’S MOST POPULAR SPORT

A. History

Soccer is the world’s most popular sport, with an estimated 3.5 to 4 billion fans worldwide. Certain estimates provide that more than 200 countries play the game of soccer, with around 265 million players actively involved in soccer around the world. According to FIFA statistics, 3.572 billion people worldwide tuned in at some point to the 2018 FIFA World Cup, with 1.12 billion people watching the final alone. The 2018 FIFA World Cup, which took place in Russia, was the most-viewed sporting tournament in history. While Americans call it “soccer,” the rest of the world refers to soccer as some translation of the two words “foot” and “ball,” with England, for example, calling the sport “football.” Although soccer is the fourth most popular sport in the United States, the sport is still growing. The professional soccer league in the United States is Major League Soccer (“MLS”). From 2013 to 2018, the MLS’s average attendance of 21,358 was the eight highest for a soccer league in the world.

B. FIFA

In French, “FIFA” stands for “Fédération Internationale de Football Association.” In English, it translates to “International Federation of Association Football.” FIFA is the world governing body of soccer, responsible for the major tournaments such as the World Cup. Established in Paris in 1904, hence the aforementioned French translation, FIFA currently has its headquarters in Zurich, Switzerland. FIFA has a complex structure, but a brief overview of

---

105 Id.
108 Id.
109 Id.
112 Id.
113 Aisling Moloney, What does FIFA stand for and when was it formed?, (Sep. 25, 2017), https://metro.co.uk/2017/09/25/what-does-fifa-stand-for-and-when-was-it-formed-6953964/ (last visited Apr. 13, 2020).
114 Id.
115 Id.
FIFA’s governing powers and organization needs to be discussed. Having an idea of how FIFA works is essential to understanding how issues relating to ABD are being addressed by FIFA.

1. FIFA’s Structure

Giovanni Vincenzo Infantino is the current president of FIFA.116 The president is elected every four years (and can be reelected)117 by representatives from member associations who are eligible to vote at the FIFA Congress, FIFA’s supreme governing body.118 The other most influential position alongside the president is the Secretary General, who is the chief executive officer (CEO) of FIFA.119 There are 211 affiliated associations to FIFA, which represent the 211 countries that are recognized by FIFA.120 Virtually every present-day country is recognized by FIFA, even including associations that are not independent countries, like Hong Kong.121 The 211 associations make up 6 confederations.122 The confederations are: the AFC in Asia, CAF in Africa, the Football Confederation (CONCACAF) in North and Central America and the Caribbean, CONMEBOL in South America, UEFA in Europe, and the OFC in Oceania.123 Simply put, the associations represent the countries (or non-independent nations) and the confederations consist of the continents where the countries reside.

2. FIFA Governing Bodies

FIFA contains a congress, council, and various committees and divisions. The FIFA Congress is the supreme and legislative body of FIFA,124 while the FIFA Council is the strategic and oversight body of FIFA.125 FIFA contains nine standing committees and four independent committees.126 According to FIFA’s explanation of the committees, “The standing committees advise and assist the Council and the general secretariat in fulfilling their duties, while the independent committees conduct their activities and perform their duties entirely independently but always in the interest of FIFA and in accordance with the Statutes and regulations of FIFA.”127 For the purposes of this article, the most important division of FIFA is the FIFA Legal & Compliance Division, which is responsible for FIFA’s legal portfolio in cases before the Court of Arbitration for Sport (CAS) or ordinary courts.”128

---

119 FIFA, FIFA Statutes, art. 37, para. 1 (2019).
120 Supra note 118.
122 Supra note 120.
123 Id.
124 FIFA, FIFA Statutes, § Definitions, para. 8 (2019).
125 FIFA, FIFA Statutes, § Definitions, para. 9 (2019).
127 Id.
3. FIFA Statutes

FIFA statutes, passed by the FIFA Congress, contain the rules and objectives of the organization and set forth the rights and duties of the President and governing bodies. The June 2019 edition of the FIFA statutes is the most current version. Every association is required to follow the statutes, and may be disciplined for violating them. In addition to the statutes, FIFA also released 2019 versions of their code of ethics and disciplinary code.

From a legal perspective, the most important statute is a FIFA Statute titled “Court of Arbitration for Sport (CAS),” which provides that “FIFA recognizes the independent Court of Arbitration for Sport (CAS) with headquarters in Lausanne (Switzerland) to resolve disputes between FIFA, member associations, confederations, leagues, clubs, players, officials, intermediaries and licensed match agents.” In addition, “CAS primarily applies the various regulations of FIFA and, additionally, Swiss law.” Because Swiss law is mainly applied in CAS proceedings involving players, an overview of Swiss law regarding privacy and data protection is needed.

C. Swiss Law

In Switzerland, data protection is mainly regulated by the Swiss Federal Data Protection Act (DPA) and the Data Protection Ordinance (DPO). The DPA contains general rules on data protection and specific regulations on data processing by private persons and federal authorities. The DPO was adopted to clarify certain aspects of the DPA provisions, for example, measures that must be taken for the cross-border disclosure of data. The DPA and DPO apply to personal data, which means all information relating to an identified or identifiable person. This means that the DPA and DPO regulate the collection of ABD.

The following is a list of relevant portions in the DPA and DPO that deal with relevant law for the purposes of this article:

- Private persons are required to register data collections if they include sensitive data or if the data is communicated regularly to third parties (Article 11a, paragraphs 2 and 3, Swiss Federal Data Protection Act (DPA)).
- Personal data processing must be carried out in good faith and must be proportionate.
- Personal data must be protected against unauthorized processing by appropriate organizational and technical measures (Article 7, DPA).
- Consent is not necessarily required for the lawful processing of personal data.

---

130 Id.
131 Supra note 127.
133 FIFA, Disciplinary Code (2019).
134 FIFA, FIFA Statutes, art. 57, para. 1 (2019).
135 Data protection in Switzerland: overview, Practical Law Country Q&A 9-502-5369.
136 Id.
137 Id.
138 Id.
139 Id.
140 Id.
141 Id.
• Consent can be implied or inferred, provided that it is given voluntarily on the provision of adequate information (informed consent).\textsuperscript{143}

• Explicit consent is required for the processing of sensitive personal data or personality profiles (\textit{Article 4, paragraph 5, Swiss Federal Data Protection Act (DPA)}).\textsuperscript{144}

• Consent is required for cross-border data disclosure in the absence of legislation that guarantees adequate protection (\textit{Article 5, paragraph 2 b, DPA}).\textsuperscript{145}

• There are no specific rules that apply to consent by minors.\textsuperscript{146}

• If consent is not given, processing can be justified by law or on the basis of an overriding private or public interest (\textit{Article 13, paragraph 1, Swiss Federal Data Protection Act (DPA)}).\textsuperscript{147}

• Generally, the data subject must be notified, or at least be made aware, of the purposes of data collection and processing, identity of the data controller, and categories of data recipients, if disclosure of data is planned.\textsuperscript{148}

• Anyone who willfully breaches professional confidentiality obligations relating to sensitive personal data or personality profiles is liable to a fine.\textsuperscript{149}

• Data subjects can file civil actions and request interim measures. Data subjects can request that data processing be stopped, no data be disclosed to third parties, and personal data be corrected or destroyed.\textsuperscript{150}

Based on the aforementioned law, regulations, and penalties, it seems that Switzerland has strict privacy regulations concerning the collection of biometric data. Although it is concerning that “[c]onsent is not necessarily required for the lawful processing of personal data,”\textsuperscript{151} there are restrictions in place. This is important to the collection of ABD because, as this article will illustrate, the FIFA Statutes and Regulations seem to be silent on the topic.

\section*{IV. THE COLLECTION OF ATHLETE BIOMETRIC DATA IN SOCCER}

\subsection*{A. ABD in Soccer}

The mass collection of ABD is becoming a common practice in soccer around the world. Whether someone is for or against the collection of ABD, this subject may be viewed from multiple perspectives. For the purposes of this article, there are three parties involved in the collection of ABD. The first party is the athlete, the second party is the athlete’s team, and third party refers to any party outside of the player-team relationship. First, this section will list some examples of devices utilized in soccer to collect ABD. Next, there will be a brief discussion of the collection of ABD from teams’ and third parties’ perspectives. Then, this section will address

\textsuperscript{142} Id.
\textsuperscript{143} Id.
\textsuperscript{144} Id.
\textsuperscript{145} Id.
\textsuperscript{146} Id.
\textsuperscript{147} Id.
\textsuperscript{148} Id.
\textsuperscript{149} Id.
\textsuperscript{150} Id.
\textsuperscript{151} Id.
what rights players have in their own ABD. Finally, this section will summarize the current views on ABD and predict how this area will develop moving forward.

1. Devices Used to Collect ABD in Soccer

In addition to the methods used today, new technology is evolving the collection of ABD. In soccer, the most common form of collecting ABD is through wearable technology worn by the players containing GPS monitors. GPS coordinates are produced by sensors within the wearable technology that measure a player’s biometric information. Common sensors include accelerometers (measuring velocity), gyroscopes (measuring orientation and rotation), and temperature sensors (measuring body temperature). One popular method is placing the GPS monitor inside the back of a bra-like garment that goes underneath a training shirt or jersey. Other popular methods of using GPS monitors to collect players’ ABD include embedding the GPS device right into a jersey, soccer cleat, sock, and fitness watch. The list seems endless because the smaller the GPS monitors get, the easier it is to embed these devices on the player.

Examples of more traditional wearable devices that collect ABD include heart rate monitors to measure heart rate, face masks with breathing valves to measure oxygen intake, and advanced x-rays used for measuring bone density. Another, less popular method teams have collected a player’s data is through tools using Radio Frequency Identification (RFID). RFID technology uses radio waves to identify people or objects by using two devices, where one device will read information contained in another wireless device or “tag” from a distance.
without making any physical contact or requiring a line of sight.\textsuperscript{165} Tools using RFID are used to collect data on players such as distance traveled, speed, and other factors.\textsuperscript{166} Data obtained from RFID is storable information that can be used to analyze individual players.\textsuperscript{167}

Besides collecting ABD from wearable technologies, soccer teams collect large quantities of ABD from nonwearable devices based on individual athletes. One example is equipment, like soccer balls with built-in sensors.\textsuperscript{168} The ball collects data on the power, spin, strike, and trajectory of the ball after being kicked, with the measurements displayed instantly.\textsuperscript{169} Another example is using a multi-camera computerized tracking system, which tracks a player’s running distance and intensity during a game.\textsuperscript{170} Finally, computerized time-motion analyses are used to study a player’s development of fatigue during matches.\textsuperscript{171} All of this data is considered ABD because it is unique to the specific athlete and can be measured.

2. How Teams Use ABD

This sub-section discusses some ways teams are using and collecting biometric data. When soccer teams use wearable technologies to collect ABD, the team usually owns at least some rights in the player’s ABD.\textsuperscript{172} Therefore, if a player transfers to another team, that player’s ABD would not be transferred unless agreed upon by the teams beforehand.\textsuperscript{173} Containing all the ABD on each of their players gives teams power because they are currently not required to share the ABD of their players with other teams.\textsuperscript{174}

As a result of this new technology streamlining the process for soccer teams to collect ABD, coaches and medical staff are able to access and collect large amounts of helpful personal player data.\textsuperscript{175} ABD is used to prevent player injuries, especially by studying data on sleep quality, workload indicators, and soreness.\textsuperscript{176} Coaches and trainers use the collected ABD to monitor player wellness and adjust training sessions accordingly.\textsuperscript{177} In addition, the ABD

\textsuperscript{166} Supra note 164.
\textsuperscript{167} Id.
\textsuperscript{168} Johnson, supra note 159.
\textsuperscript{169} Id.
\textsuperscript{172} Calistri, supra note 156.
\textsuperscript{173} Id.
\textsuperscript{174} Id.
\textsuperscript{175} Id.
\textsuperscript{177} Calistri, supra note 173.
collected provides the opportunity for specific feedback to each individual player, which can be used in a game setting.

3. Third Party Use of ABD

One way a third party can gain access to a player’s ABD is through third-party ownership of soccer players. This is when a third party, such as a company or an agent, owns all or part of the financial rights to a player. This practice has been criticized by soccer journalists because it is in the third party’s best interest to sell the player as often as possible to generate more money from the player transferring teams. Influential figures in soccer have labeled the third-party ownership of soccer players as a form of modern-day “slavery.” Third-party ownership of soccer players was banned by the Premier League (the highest division of soccer in England) in 2008 because it concluded third party ownership “raises too many issues over the integrity of competition” and “the development of young players.” Although this type of third-party ownership commonly deals with a player’s financial rights related to transfers, this shows how third parties have the capability to financially exploit players by owning their ABD.

Third parties also include the vendors or manufacturers that supply the biometric equipment and incident services. It is common for companies that supply biometric collection equipment to store the data their devices collect on company servers. As discussed earlier, these companies may face civil penalties (i.e., BIPA violations) without proper disclosure and consent from the individual whose biometric data is being collected. Companies need to understand what rights and responsibilities they owe the player, as well as the business relationship that exists with their client.

Finally, third parties collect ABD for entertainment purposes. Examples of third parties that possess large amounts of ABD in the entertainment industry include, but are not limited to, fantasy sports, gambling, and video game companies.

a. Fantasy Sports/ Gambling

ABD has the potential to be used in fantasy sports and sports betting. An example is the Alliance of American Football (AAF), a league that plays American Football in the United

---

178 *Id.*
180 *Id.*
181 *Id.*
182 *Id.*
183 *Id.*
States. Before the AAF went bankrupt, the league sold the rights to their players’ ABD in a partnership with MGM Gaming. The AAF was planning on having their players use wearable technologies to collect ABD, which would be used in conjunction with a mobile app that would allow the better to place wagers during the game with odds that are directly influenced by the readings of the biometric stats. Although it is unclear how involved soccer teams are with fantasy sports and the gambling industry, the availability of these types of deals is becoming increasingly prevalent in the sports world.

b. Video Games

The FIFA soccer video game, the Guinness World Record holder for the best-selling videogame sports series with around 200 million units sold, has been using “real-world” data from players for years. In addition to ABD, videogame companies are running into issues when they collect user biometric data as well. A class action lawsuit was filed against the NBA 2K video game franchise, because the games were using face-scanning technology to create playable avatars. Video games are another way the entertainment industry can be involved and potentially liable for possessing an athlete’s ABD.

B. Player Rights in Their Own ABD

On a preliminary note, it is important to point out FIFA’s overwhelmingly positive attitude towards wearable technologies that collect a soccer player’s ABD. FIFA mainly refers to these wearable technologies as Electronic Performance and Tracking Systems (“EPTS”). FIFA defines EPTS as “technologies used to monitor and improve player and team performance.” EPTS “primarily tracks player (and ball) position, but can also be used in combination with microelectromechanical devices (accelerometers, gyroscopes, etc.) and heart-rate monitors, as well as other devices to measure load or physiological parameters.” Catapult, a company that produces wearable technologies that collect ABD, became the first provider to have its technology approved for in-game use by FIFA according to the federation’s International Match Standard (IMS) for Electronic Performance and Tracking Systems.

---

189 Id.
193 Id.
195 Id.
196 Id.
197 Catapult, CATAPULT TECHNOLOGIES BECOME FIFA-APPROVED WEARABLE TRACKING DEVICES,
In 2017, FIFA launched the FIFA Quality Programme for EPTS, with the goal “of ensuring that wearable tracking systems used in football do not pose a danger to the players.”\(^{198}\) The FIFA Quality Programme also “aims to provide guidance to competition organizers [sic] when appointing a provider of tracking systems for their competition.”\(^{199}\) Even though wearable technologies are a recent development, FIFA already has a specific program in place to teach competition organizers how to safely implement EPTS. FIFA also organizes dates for EPTS testing, where EPTS providers interested in getting their systems certified by FIFA are able to get their systems tested.\(^{200}\)

For a company’s ETPS to be used in a soccer match, the wearable device must meet the International Match Standard (“IMS”) as set out in the FIFA Quality Programme for Wearable Electronic Performance and Tracking Systems.\(^{201}\) The IMS standard in the FIFA Quality Programme states that when EPTS “are used (subject to the agreement of the national football association/competition organizer [sic]): they must not be dangerous [and] information and data transmitted from the devices/systems is not permitted to be received or used in the technical area during the match.”\(^{202}\) The IMS standard is broad and lacks any description of how the ABD will be used. It only provides that the data cannot be “received or used in the technical area during the match.”\(^{203}\) This may be used to prevent cheating by forbidding ABD collection in certain areas during a match. The IMS standard broadly addresses player safety by stating that the EPTS systems cannot “be dangerous,” but there is no mention of how the player’s legal rights will be implicated or what is being done in order to avoid liability.\(^{204}\)

The FIFA Statutes are not clear in determining what rights players have regarding their own ABD after it is collected. A FIFA Statute titled “Players,” provides that “[t]he Council shall regulate the status of players and the provisions for their transfer, as well as questions relating to these matters, in particular the encouragement of player training by clubs and the protection of representative teams, in the form of special regulations from time to time.”\(^{205}\) A plain reading of this statute does not offer much. It is overly broad and, on its face, seems to give the Council a significant amount of power over the players. The FIFA Statutes emphasize the rules and organization of soccer on a worldwide scale instead of a player’s individual rights.

Another FIFA Statute that is broadly worded but has the potential to involve the collection of a player’s ABD is a statute titled “Rights in competitions and events,” which provides the following:

\(^{199}\) Id.
\(^{203}\) Id.
\(^{204}\) Id.
\(^{205}\) FIFA, FIFA Statutes, art. 6, para. 1 (2019).
1. FIFA, its member associations and the confederations are the original owners of all of the rights emanating from competitions and other events coming under their respective jurisdiction, without any restrictions as to content, time, place and law. These rights include, among others, every kind of financial rights, audiovisual and radio recording, reproduction and broadcasting rights, multimedia rights, marketing and promotional rights and incorporeal rights such as emblems and rights arising under copyright law.

2. The Council shall decide how and to what extent these rights are utilised and draw up special regulations to this end. The Council shall decide alone whether these rights shall be utilised exclusively, or jointly with a third party, or entirely through a third party.”

Although this statute does not specifically reference “data,” it labels FIFA as the “original owners” of all content from competitions. Once again, on the face of this statute, it seems to grant FIFA a broad discretion of power and does not reference the athlete. Data used from the collection of ABD during a competition is “content.” For example, a broadcast of a soccer game will show the distance a player has run throughout the game. This statistic is obtained from the collection of a soccer player’s ABD, most likely from wearable technology they are wearing during the game. The FIFA Statutes seem to grant FIFA the authorization to use the athlete’s ABD. For example, a FIFA Statute titled “Authorisation to distribute,” provides the following:

“1. FIFA, its member associations and the confederations are exclusively responsible for authorising the distribution of image and sound and other data carriers of football matches and events coming under their respective jurisdiction, without any restrictions as to content, time, place and technical and legal aspects.

2. The Council shall issue special regulations to this end.”

Once again, the players seem to be lost in the shuffle in relation to the collection of their ABD. One last FIFA Statute to reference is a FIFA Statute regarding the Medical Committee, which provides that “The Medical Committee shall deal with all medical aspects of football, including the fight against doping.” The collection of ABD has many medical implications and disclosure requirements, but the FIFA Statutes are only concerned with players “doping,” which refers to players cheating by taking banned substances.

In conclusion, there seems be a pattern with the FIFA Statutes, Regulations, and Guidelines granting broad power to the FIFA governing bodies and not the players. Surprisingly, information regarding players’ rights in their ABD are difficult to find, and quite simply put, there is not much available. One explanation regarding this lack of information is the recent introduction of wearable technologies into the sport of soccer. Another is that FIFA, a worldwide organization, understandably needs to delegate legal problems and issues to the specific confederations and countries. Numerous legal concerns and issues are arising because of the minimal regulation of the collection of ABD in soccer. The next section introduces some of these legal concerns and issues.

207 FIFA, FIFA Statutes, art. 68, para. 1-2 (2019).
208 FIFA, FIFA Statutes, art. 48, para. 1 (2019).
1. Legal Concerns and Issues with the Collection of ABD

As previously discussed, legal issues concerning the collection of ABD involve three parties.209 The first party is the athlete, whose data is being collected.210 The second party is the institution that wishes to use the data, typically the athlete’s team.211 The third party is the vendor or manufacturer that provides the biometric equipment and services.212 For each party, the legal issues are different, but there are overlapping similarities. While this article discusses how teams and third parties are involved in the collection of ABD, the focus of this article is on the legal issues from the athlete’s perspective. This article consists of four legal topics associated with the collection of an athlete’s ABD: consent, privacy, publicity rights, and contract disputes. The purpose of the next sections is to introduce the specific legal issues and the concerns created in relation to the collection of an athlete’s ABD.

a. Consent

Consent spans a variety of legal areas and is a crucial factor in the legal implications of the collection of ABD. Attorney Kristy Gale represents athletes and has helped athletes protect their interests in their own ABD.213 In a phone interview with Gale for this article, Gale spoke to the importance of obtaining an athlete’s consent when collecting the athlete’s ABD.214 Gale stated, “It’s all about consent. That’s the most important issue. Athletes need to understand what consent means under the law and how that could impact them, their career, their play time, and their monetary compensation.”215 When proper consent is lacking, an athlete’s ABD can be used for someone’s financial gain without the athlete’s knowledge.

Consent is defined as an “[a]greement, approval, or permission regarding some act or purpose, esp. given voluntarily by a competent person.”216 Consent can be expressed or implied. Express consent is clearly and unmistakably stated.217 Implied consent is inferred from one’s conduct rather than from one’s direct expression, or, stated differently, “imputed as a result of circumstances that arise.”218 Informed consent is defined as a “person’s agreement to allow something to happen, made with full knowledge of the risks involved and the alternatives.”219 As pointed out earlier in BIPA, statutes define informed consent.

When players sign a contract, it is inevitable that they will give up certain rights to the team they play for. But what is included in the rights the players are signing away? A problem arises when players think they are giving up certain rights in one category, but in reality, they are giving away rights in a different one. Lines may be blurred as to what is considered ABD with ABD being a relatively recent concept. Do players really know what they are consenting to? With FIFA’s support of wearable technologies, are soccer contracts starting to define biometric

---

209 Mintz, supra note 184.
210 Id.
211 Id.
212 Id.
215 Id.
217 Id.
218 Id.
219 Id.
data and explain how it will be collected? These are a few basic questions related to consent that need to be discussed with the growing use and collection of ABD.

Another consent issue to discuss is regarding the consent of minors. Some soccer players on the world’s biggest clubs are under the age of 18, and there are different issues regarding minors and the use of their ABD. When consent is given by parents on behalf of minors, they should be informed about the collection of their child’s ABD. A parent’s ability to consent on behalf of their child, along with general rights of minors, differ from country to country. FIFA regulations address the international transfer of minors, but lack substantive information related to consent in general.

Finally, teams and other third parties can use consent as an affirmative defense. For example, consent is used as a common defense for invasion of privacy. Because consent can be used against them, athletes need to be aware of what they are consenting to when they sign their contracts. Consent is important for all parties involved, especially the athlete because it is his/her ABD that is potentially being financially exploited.

b. Privacy

One major legal concern of collecting an individual player’s ABD involves the player’s privacy rights. The Restatement (Second) of Torts provides that there are four ways an individual’s right of privacy may be invaded. They are: (1) unreasonable intrusion upon the seclusion of another; (2) appropriation of the other’s name or likeness; (3) unreasonable publicity given to the other’s private life; and (4) publicity that unreasonably places the other in a false light before the public. The collection of an athlete’s ABD has the potential to affect each of these categories because an athlete’s ABD contains sensitive information, unique to the individual athlete.

Unreasonable intrusion upon the seclusion of another “consists solely of an intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man.” An example of this would be an athlete’s medical information. ABD contains an athlete’s sensitive medical information, which, in many circumstances, the athlete would like to keep private. Personal medical biometric information is protected by the Health Insurance Portability and Accountability Act (HIPAA), in addition to state statutes like the Illinois Personal Information Privacy Act.

---

223 Restatement (Second) of Torts § 652A (1977).
224 Restatement (Second) of Torts § 652B (1977).
226 Id.
Appropriation of the other’s name or likeness is when someone “appropriates to his own use or benefit the name or likeness of another...”227 A common form of this appropriation is use of an athlete’s name or likeness to advertise the violator’s business or product, or for some similar commercial purpose.228 This is the most typical form of privacy invasion that occurs when an athlete’s ABD is collected. Misappropriation is a common-law tort “for using the noncopyrightable information or ideas that an organization collects and disseminates for a profit to compete unfairly against that organization, or copying a work whose creator has not yet claimed or been granted exclusive rights in the work.” An athlete’s ABD is originally the athlete’s property. If the athlete has not given consent for someone to use his/her ABD, and his/her ABD is used for profit or in a manner the athlete was unaware of, the athlete may have a misappropriation claim. For example, say a sports betting company used an athlete’s ABD to set the odds for bets a customer can place. The company is strategically setting the odds in a way that will be most profitable. Is the athlete aware that their collected ABD is being used to set betting lines for a profit? The answer is most likely no.

The third invasion of privacy, unreasonable publicity given to the other’s private life, involves someone giving publicity to a matter concerning the private life of another.229 A person will be liable for this type of invasion of privacy if the matter publicized is of a kind that would be highly offensive to a reasonable person and is not of legitimate concern to the public.230 This is another likely claim an athlete may make. Unreasonable publicity can involve the disclosure of embarrassing facts that an athlete hoped to keep private. For example, someone could use an athlete’s ABD, like biometric data related to heart health, to project that an athlete will have a short career. If published, this information has the potential to affect a soccer player’s contract negotiations. The average male professional soccer player is considered to be in his prime at an early age, peaking between the ages of 25 and 27.231 In the wrong hands, the unauthorized disclosure of an athlete’s ABD can negatively affect a soccer player’s career.

Finally, a person can be liable for publicity that unreasonably places the other in a false light before the public. Liability is found if the false light would be highly offensive to a reasonable person, and the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.232 Similar to the example above with a third party using an athlete’s ABD to project the length of their career, the collected ABD can be manipulated to reach false conclusions, putting the soccer player in a false light.

On a final note related to privacy, the U.S. Soccer and FIFA privacy statements/policies for their websites have an interesting distinction. The U.S. Soccer privacy statement provides “[e]xcept as expressly disclosed above as to information about race and ethnicity, we do no collect “special categories” of Personal Data about you (this includes… genetic and biometric data).”233 The FIFA privacy policy does not mention biometric data.234 Although this is not

---

227 Restatement (Second) of Torts § 652C (1977).
228 Id.
229 Restatement (Second) of Torts § 652D (1977).
230 Id.
directly related to the collection of ABD, this shows that the U.S. is becoming more aware of the potential dangers of collecting anyone’s biometric data.

c. Publicity Rights

There are a variety of intellectual property rights an athlete must be aware of, but this section will focus on an athlete’s publicity rights. The right of publicity prevents the unauthorized commercial use of an individual’s name, likeness, or other recognizable aspects of one's persona.235 The right of publicity gives an athlete the exclusive right to license the use of their identity for commercial promotion.236 The right of privacy and the right of publicity can be hard to differentiate, and both seem to share overlapping legal issues. Although the distinction is complex, some have simply stated that privacy rights deal with personal rights while publicity rights deal with property rights.237 Courts have stated that the right of publicity is “an outgrowth of the right of privacy.”

Even though there is no clear list of what publicity rights entail, courts have held that performance statistics239 and voice240 constitute publicity rights that are afforded protection. As Kristy Gale points out, ABD is a publicity right because of the unique biological and behavioral characteristics that comprises an athlete’s ABD.241 Athletes need to be aware of how the collection of their ABD can violate their publicity rights. A soccer player’s publicity rights can be violated when his/her ABD is used in broadcasts, team promotions, video games, fantasy sports, gambling, and other commercial purposes. In many instances, athletes may be entitled to damages if their ABD is used without compensation. Finally, teams collecting their players’ ABD also need to be well-versed in an athlete’s publicity rights, which helps teams understand how they can and cannot use a player’s ABD, in addition to when an athlete should be compensated for the use of their ABD.242

d. Contract Disputes

The collection of an athlete’s biometric data has the potential to affect their contract negotiations. Consent, privacy rights, and publicity rights all play a part in contract negotiations. When an athlete agrees to a contract, the athlete’s consent, whether express or implied, grants the team a variety of powers. How much power is granted to the teams regarding the athlete’s privacy and publicity rights? Privacy rights may be violated if the team discloses an athlete’s personal information. Publicity rights may be violated if the team uses the athlete’s ABD without compensating the athlete. Privacy and publicity rights that an athlete consents to sign over to a team can be used to negotiate a player’s salary.

236 Id.
241 Gale, supra note 152.
242 Supra note 222.
There are dangers associated with a team possessing an athlete’s ABD. Because ABD is unique to each individual soccer athlete, it can be used to exploit the athlete during contract negotiations. For example, teams could use an athlete’s ABD as leverage for a lower salary because his/her ABD demonstrates that he/she becomes fatigued earlier than other players on said team, therefore costing this player a significant monetary loss. On the other hand, athletes could use their ABD related to health or past injuries to argue that they deserve more money because they are less likely to get injured than other players on the team. Either way, an athlete’s ABD can have a tremendous effect, especially when contract negotiations are concerned.

As Gale points out, “The primary issues [for contract disputes] will come down to the definition of data and the definition of how that data may be used, either under the collective bargaining agreement or individual player contracts.”

It is crucial for the athlete to be aware of how teams are defining and using their ABD. One place to start is in collective bargaining agreements. Collective bargaining agreements (“CBAs”) are used in sports to negotiate player rights between the players and the teams. Generally, a collective bargaining agreement is a written legal contract between an employer and a union representing the employees. FIFA uses CBA’s, but allows the different associations to address legal issues individually. CBA’s have a part in governing the collection and use of ABD. Generally, it seems that CBAs, along with other standard player contracts, allow broad collection and use of athlete health-related data. The last CBA between Major League Soccer and the Major League Soccer Players Union, however, did not reference “biometric data,” or even “data” in general. There is a new tentative CBA in effect, but it is still unknown if it references the collection of ABD. CBAs should be an important contractual tool used to address the collection of ABD. As the popularity of teams collecting ABD increases, future CBAs will need to address how to regulate and incentivize the collection of ABD.

C. Big Picture of ABD Collection

The future of ABD collection is hard to predict. As discussed throughout this article, technology will continue to develop and the law will have to adapt. There are multiple parties involved with this issue, and arguments can be made from both sides on whether the mass collection of ABD is helping or hurting the athlete. The following two sections address some of the pros and cons associated with the collection of ABD in soccer.

---

247 Id.
1. Pros

Some pros involved with the mass collection of ABD include injury prevention, player safety, added incentives, fan engagement, increased viewer content, and enhanced viewer experiences.

From a player’s perspective ABD can help injury prevention, player safety, and add incentives. Technology used to collect the athlete’s ABD has the potential to catch injuries before they happen. Certain ABD technologies that track a player’s physical characteristics can show if a certain part of the body is weaker or starting to develop an injury, and even potentially uncover an unknown heart condition. ABD could also be used to test how players react to certain surfaces and be used to design safer playing fields. In terms of contract negotiations, an argument can be made that an athlete’s ABD could help demonstrate the athlete’s value. For example, an athlete can argue that his/her ABD shows he/she is more valuable than what traditional statistics would suggest. Finally, an athlete’s ABD can have monetary effects. If the athletes give consent and are properly compensated for the use of their ABD, it could become a large source of income for the athletes.

From a soccer fan’s perspective, the collection of ABD increases fan engagement, develops more content, and enhances the viewership experience. Fans have access to their favorite players’ strengths and weaknesses when their ABD is collected. ABD adds content for sports entertainment and gaming, like fantasy sport platforms. Finally, with all of the additional statistics provided from the collection of ABD, live viewing of sporting events enhances the viewer’s overall experience.

Finally, in relation to wearable technology, FIFA’s official release on the Electronic performance and tracking systems lists the following benefits for the devices:

- Non-invasive to players
- Commonly used in the football market
- High sampling rate, ball tracking possible
- High number of measurements possible
- Accuracy of measured data in real-time
- Ultra-wide band technology reduces chances of interference in transmission path
- Short installation time
- Operator not needed

2. Cons

As illustrated with the various legal issues discussed throughout this article, the major concerns associated with the collection of ABD involve the athlete’s privacy rights, publicity rights, and potential financial exploitation. If athletes do not consent to the use of their ABD, personal rights can be violated by private information being released, publicity rights can be violated by the unauthorized use of an athlete’s biometric data for commercial gain, and an athlete can lose leverage in their contract negotiations.

---

Data monetization, which is the process of using data to increase revenue,\textsuperscript{251} may be the biggest proponent of athlete financial exploitation. Gale has advocated for protecting athletes’ rights when their data is being monetized.\textsuperscript{252} In terms of the danger, Gale stated the following:

“The athlete is not aware that the data collected from them can be used to make money. It can be used for sports betting. Leagues and teams could collect the data for one purpose, to help the athlete perform better or train better, but then later use that data for a business purpose, for example, pushing it out for sports betting or fantasy sports or push out to virtual reality or content creators, whatever that looks like, athletes aren’t aware of that. That’s the biggest issue, athletes being exploited.”\textsuperscript{253}

With the numerous uses that an athlete’s ABD can have, athletes must be aware of the potential dangers associated with the collection of their ABD. Education for athletes is key. The more the athlete knows about how his/her ABD is being collected and used, the higher the probability of the athlete making an informed decision on what rights teams and third parties should have in his/her ABD.

3. Possible Solutions

One thing is for certain; the mass collection of ABD will continue in every sport. For soccer, especially with FIFA’s support and enthusiasm for wearable technologies, the collection of ABD should grow faster than in other sports. As this article illustrated, there are many parties involved and legal concerns associated with the collection of ABD. It is hard to predict how this area will be addressed and regulated in the near future. Two foundational requirements that need to be implemented in the collection of ABD are consent and disclosure.

a. Importance of Consent

As pointed out earlier, consent involves many legal questions that are yet to be determined. First, and most importantly, athletes need to give informed consent to teams and third parties so their ABD may be collected. Next, players need to give informed consent to where their ABD can be sent and who can possess it. Finally, athletes need to give informed consent so their ABD can be used in the ways that teams and third parties have intended. As Gale points out, consent is the most important issue.\textsuperscript{254}

b. Need for Disclosure

After receiving an athlete’s consent, there should be specific disclosure requirements that teams and third parties are forced to abide by with regards to collecting ABD. First and foremost, teams and third parties must disclose to the athlete that their ABD is being collected. This article suggests the following three requirements of disclosure teams and third parties should provide to athletes when their ABD is collected: (1) Definition; (2) Dissemination; and (3) Use.

\textsuperscript{252} Telephone Interview with Kristy Gale, Attorney, (Mar. 20, 2020).
\textsuperscript{253} \textit{Id.}
\textsuperscript{254} \textit{Id.}
First, teams need to define what an athlete’s ABD consists of, either in the athlete’s contract or a separate disclosure agreement. This is still a developing area of law, and teams need to look at relevant statutes and regulations to see how biometric data is defined. Soccer is an international sport where players constantly transfer to teams located in different countries. Biometric data definitions and regulations will vary from country to country. In the United States, for example, definitions and regulations concerning the collection of biometric data differ across each state. Regardless, each time an athlete signs a new contract with a team, biometric data should be defined.

Furthermore, teams need to disclose to the athlete how their ABD will be disseminated. The athlete needs to know who will be in possession of their ABD. Teams have numerous agreements containing large financial implications with entertainment companies for matters such as broadcasting rights and fan engagement. Athletes must be informed to which companies their respective teams are selling their ABD. In addition, athletes need to be aware of which vendors and manufacturers that produce wearable technologies are in possession of their ABD. Are these vendors storing the athlete’s ABD or deleting that data once given to the team? Who has the burden of disclosing that information to the athlete? The burden would most likely be on the team, however, the team may not know what vendors are doing with the ABD after it is collected. It should be the team’s responsibility to uncover what the vendors are doing with the collected ABD. Teams, in their agreements with vendors, should explicitly state whether they prefer the vendors to delete or store the collected ABD. Regardless, teams need to know what vendors are doing with the collected ABD to properly inform athletes who is possessing their ABD.

Finally, teams and third parties need to disclose the use of the athlete’s ABD. A major concern with the mass collection of ABD is the concern of financial exploitation by teams and third parties using an athlete’s ABD. Another concern deals with potential violations of an athlete’s privacy rights. To prevent financial exploitation and protect privacy rights, full disclosure of how an athlete’s ABD will be used is necessary. How will the team use the athlete’s ABD? Will the team mainly use the ABD for injury prevention or game strategy? How will third-party companies involved in broadcast or fantasy sports use the athlete’s ABD? Will an athlete’s ABD be used solely for live game analysis or will it also be used for future fan engagement programs? Will the athlete’s ABD be used for fantasy sports projections or will it also be sold to gambling companies for setting odds? These are just a few of the potential many questions, and the list may seem never-ending, but the athlete should be informed and have the opportunity to ask how their ABD is used. Even though full disclosure of how an athlete’s ABD is used may be a nuisance for teams and third parties, the athlete has a legal right to that information.

Like many commentators in this area, athletes also have their own perspectives and opinions about the collection of their ABD. Full disclosures related to what ABD is collected, who is possessing the ABD, and how ABD is used are crucial pieces of information necessary to be given to athletes so they can form their own educated opinions.
V. CONCLUSION

The purpose of this article is to provide an overview of certain legal issues that arise out of the mass collection of ABD in soccer. The goal was to provide the reader with a neutral perspective, so that the reader can form their own opinion on whether this is good or bad for soccer. Whether on one side of the argument or the other, this article gave you a sense of the pros and cons associated with the collection of ABD. A main focus of this article was the importance of athlete awareness. Regardless of how this area evolves, athletes need to give informed consent and receive proper disclosure as to when their ABD is collected and how it will be used. Whether through legislation or player initiative, athletes will become more aware of the rights they have in their own ABD. The collection of ABD will continue to become an integral part of soccer.