

THE MONETIZATION OF ATHLETE BIOMETRIC DATA IN LESS CENTRALLY REGULATED PROFESSIONAL SPORTS—A NEW REVENUE STREAM OR A DATA PRIVACY NIGHTMARE?

Raul J. Muniz[†]

INTRODUCTION

In 2020, more than 400 current and former soccer players in the Premier League, English Football League, National League, and Scottish Premiership threatened legal action against gambling, betting, and data processing companies over the use and monetization of player performance data and related statistics.¹ The players argued, among other things, that they did not consent to the sale of their data and that they were never presented with an opportunity to be compensated for the use of their data.² Although their claims are based on the European Union's General Data Protection Regulation,³ similar issues may arise in the context of professional sports here in the United States.

That said, data is the new oil, and when refined, it can be used to predict athletic performance.⁴ Quite naturally, then, data analytics are advantageous in professional sports where athletes, coaches, and teams are looking to outperform the competition.⁵ There are also opportunities for athlete biometric data to be a source of revenue by licensing or selling player data to fantasy sports leagues, sportsbook companies, broadcasters, and health and fitness companies.⁶ For example, in 2018, Pro Fighters League, an American mixed martial arts

[†] Third-year law student at St. John's University School of Law.

¹ Nick Hartley & Philip Marsh, *Russell Slade: Ex-manager Leads Lawsuit over Use of Players' Personal Data*, BBC SPORT (July 28, 2020), <https://www.bbc.com/sport/football/53557706>.

² *Id.*

³ *See id.*; *see also* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. (L 119) 1.

⁴ David Jarvis et al., *The Hyperquantified Athlete: Technology, Measurement, and the Business of Sports*, DELOITTE INSIGHTS (Dec. 7, 2020), <https://www2.deloitte.com/xe/en/insights/industry/technology/technology-media-and-telecom-predictions/2021/athlete-data-analytics.html>.

⁵ *Id.*

⁶ *Id.*; *see also infra* note 9 and accompanying text.

(“MMA”) promotional company, partnered with SportsMEDIA Technology to create a SmartCage that will measure MMA fighter performance analytics along with biometric and positional data in real-time.⁷ Metrics will include the speed of punches and kicks, power of punches ratings, heart rate tracking, and energy exerted.⁸ The SmartCage fight data and analytics will also offer prop bets and gaming opportunities.⁹

There are, however, still significant questions that surround the monetization of athlete biometric data. With the emergence of data privacy laws in the United States and around the globe, terms surrounding the collection of biometric data will continue to be a point of negotiation in professional sports as the use of wearable devices increases.¹⁰ This article will discuss the data privacy implications of monetizing athlete biometric data in less centrally regulated professional sports in the United States, such as boxing, MMA, and “eSports,” where there is a high likelihood of extreme disparities in bargaining power between athletes and sports

⁷ *The PFL Continues to Reimagine MMA with Launch of the First-Ever SmartCage for 2019 season*, PROFESSIONAL FIGHTERS LEAGUE NEWS (Dec. 17, 2019), <https://www.pflmma.com/news/pfl-continues-to-reimagine-mma-with-launch-of-the-first-ever-smartcage-for-2019-season>.

⁸ *Id.*

⁹ *Draft Kings Named First Official Sportsbook And Daily Fantasy Partner of The Professional Fighters League*, PROFESSIONAL FIGHTERS LEAGUE NEWS (Apr. 20, 2021), <https://www.pflmma.com/news/draftkings-named-first-official-sportsbook-and-daily-fantasy-partner-of-the-professional-fighters-league>. Other examples include the Professional Squash Association 2018 partnership with a private biometric data collection entity to enhance the fan experience by providing real-time biometric data on the athletes while in-game. Mary Bates, *The Rise of Biometrics in Sports*, IEEE PULSE (June 28, 2020), <https://www.embs.org/pulse/articles/the-rise-of-biometrics-in-sports/>. The goal was to give fans a better understanding of the squash players’ athleticism, as well as to create more excitement around gameplay generally. *Id.* As part of the partnership deal, the athlete’s biometric data was also made available to sportsbook companies, with any revenue generated to be shared among the league, players, and partners. *Id.* Additionally, in the world of “eSports,” several leagues allow wearable devices to track eye movement and heart rate data, and fans can view those metrics on screen in real-time. Mitch Reames, *EDGE Wearable Aims to Improve Cognitive Performance in ESports*, SPORTTECHIE (Aug. 2, 2018), <https://www.sportstechie.com/edge-wearable-aims-to-improve-cognitive-performance-in-eSports/>. These metrics assist athletes, who are usually younger than 18, to reduce burnout by measuring cognitive patterns and stress levels. *Id.* Wearable devices present a separate issue of parental consent in eSports, where players are usually younger than 18. *ESports Face Significant Legal Risk Over the Collection and Use of Biometric Data*, SPORTTECHIE (Nov. 19, 2019), <https://www.sportstechie.com/eSports-legal-risk-collection-use-biometric-data/>.

¹⁰ *US State Privacy Legislation*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/> (last visited Feb. 11, 2022); *Global Comprehensive Privacy Mapping Chart*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS <https://iapp.org/resources/article/global-comprehensive-privacy-law-mapping-chart/> (last visited Feb. 11, 2022).

entities due to the lack of a comprehensive regulatory structure, player unions, and collective bargaining agreements. Further, this article will argue that the regulation of monetizing biometric data in less centrally regulated sports should be uniform and that the most effective way to accomplish substantive uniformity is for sports regulatory bodies to enact rules regulating biometric data collection themselves, as opposed to the federal government or individual states stepping in.

Section I provides a brief background on biometric data and its implementation in sports. Section II offers an overview of the regulatory regimes in professional boxing, MMA, and eSports. Section III surveys some of the current data privacy laws in the United States and discusses what laws, if any, protect athletes. Section IV details how to reach uniformity in the context of less centralized sports, where extreme disparities in bargaining power exist.

I. BIOMETRIC DATA IN THE CONTEXT OF SPORTS

Biometric data generally relates to “the measurement and analysis of unique physical or behavioral characteristics” and can be used as a means of verifying identity.¹¹ Physiological biometrics, which relate to the body specifically, include, among other things, heart rate, temperature, blood sample analysis, and facial, retinal, or iris measurements.¹² Behavioral biometrics refer to the measurement and recording of human behaviors that include, among other things, an individual’s specific movements and actions.¹³ In today’s day and age, there are new innovations in biometric data analytics thanks to the advancement of wearable devices.¹⁴ An

¹¹ *Biometrics*, MERRIAM-WEBSTER, <https://www.merriam-webster.com/dictionary/biometrics> (last visited Feb. 17, 2022). Biometric data has a legal definition under respective state laws. *See The Evolution of Biometric Data Privacy Laws*, BLOOMBERG LAW (Nov. 4, 2021), <https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/>.

¹² *State Biometric Privacy Legislation: What You Need to Know*, THOMPSON HINE, (Sept. 5, 2019), <https://www.thompsonhine.com/publications/state-biometric-privacy-legislation-what-you-need-to-know>.

¹³ *Id.*

¹⁴ David Jarvis et al. *supra* note 4.

athlete can decrease injuries, improve in-game performance, and predict future performance by analyzing their biometric data.¹⁵ The collection of biometric data typically involves a three-way relationship: (1) the athlete whose data is being collected; (2) the institution or entity (e.g., the league or the team) which wishes to use the data; and (3) the vendor that provides equipment that collects athlete biometric data (e.g., a wearable device that can track an athlete’s activity).¹⁶

As previously mentioned, creative uses of athlete biometric data can also be a revenue source by monetizing the data, such as licensing or selling the data to various sports-related entities, like fantasy sports leagues, sportsbook companies, broadcasters, and health and fitness companies.¹⁷

II. OVERVIEW OF REGULATORY REGIMES IN PROFESSIONAL BOXING, MMA, AND eSPORTS

Centralized sports, such as many of the major “American sports”—i.e., the National Basketball Association, National Football League, Major League Baseball, and National Hockey League—consist of one league and several teams that employ athletes. Additionally, these leagues have player unions that negotiate collective bargaining agreements on behalf of the athletes, including the terms surrounding the collection of biometric data.¹⁸

Unlike the other major American sports, boxing, MMA, and eSports pose unique issues due to the lack of comprehensive regulatory structures, player unions, and collective bargaining

¹⁵ *Id.*

¹⁶ Ayisha McHugh, *On Federalism and Biometrics: The Balance of Privacy and Proprietary Rights Following Murphy v. NCAA*, COLUMBIA J. OF TRANSNAT’L L. (Mar. 11, 2020), <https://www.jtl.columbia.edu/bulletin-blog/on-federalism-and-biometrics-the-balance-of-privacy-and-proprietary-rights-following-murphy-v-national-collegiate-athletic-association-ncaa>.

¹⁷ *See supra* notes 6–9 and accompanying text.

¹⁸ *See NBPA-NBA Collective Bargaining Agreement* (Jan. 19, 2017), <https://cosmic.s3.imgix.net/3c7a0a50-8e11-11e9-875d-3d44e94ae33f-2017-NBA-NBPA-Collective-Bargaining-Agreement.pdf>. The National Basketball Association’s collective bargaining agreement provides that no player data collected may be available to the public or used for any commercial purpose. *Id.* at 361; *see also WHOOP Strikes Landmark Deal as the Officially Licensed Recovery Wearable of the NFL Players Association*, BLOOMBERG (Apr. 24, 2017), <https://www.bloomberg.com/press-releases/2017-04-24/whoop-strikes-landmark-deal-as-the-officially-licensed-recovery-wearable-of-the-nfl-players-association>. Through the National Football League Player Association’s agreement between the NFL and WHOOP, players have the right to sell their data through a licensing program. *Id.*

agreements. There is no centralized league responsible for sanctioning boxing or MMA events, nor do unions or collective bargaining agreements exist to represent the interests of the athletes. Instead, several individual promoters hold events. Further, professional boxing and MMA events are regulated by different state commissions in the United States, which have different rules and regulations.¹⁹ Similarly, the rapidly growing eSports industry does not have a regulatory body in the United States.²⁰ Instead, there are loosely organized associations that sanction eSports events.²¹ No league oversees the sport, and player unions and collective bargaining agreements are likewise non-existent.²²

In conclusion, major sports in the United States have player unions that advocate on behalf of athletes and enter into collective bargaining agreements with their respective employers, which give the athletes control over certain aspects of their profession, including their biometric data. Conversely, athletes in less centrally regulated sports such as boxing, MMA, and eSports may enter into less than favorable contract agreements and ultimately have less control due to the lack of player unions and collective bargaining agreements.

III. DATA PRIVACY AND BIOMETRIC REGULATORY REGIMES IN THE UNITED STATES

The United States does not have a uniform federal regulatory system that governs personal data collection, let alone biometric data.²³ Instead, federal data privacy laws regulate specific sectors and data types.²⁴ For example, the Fair Credit Reporting Act regulates personal

¹⁹ *ABC Regulatory Guidelines*, ASSOCIATION OF BOXING COMMISSIONS (July 27, 2005), <https://www.abcboxing.com/abc-regulatory-guidelines/>. Each state reserves the right to enact its own rules and regulations to regulate professional boxing and MMA events held in their respective states.

²⁰ Jas Purewal and Isabel Davies, *The eSports Explosion*, AMERICAN BAR ASSOCIATION (Nov. 16, 2016), https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2016-17/november-december/eSports-explosion-legal-challenges-opportunities/.

²¹ *Id.*

²² *Id.*

²³ Thorin Klowsowski, *The State of Consumer Data Privacy Laws in the US (and Why It Matters)*, NEW YORK TIMES (Sept. 6, 2021), <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/>.

²⁴ *Id.*

information collected by consumer reporting agencies, and the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) regulates health information disclosed to healthcare providers and healthcare businesses.²⁵

On its face, HIPAA seems to be implicated by professional sports teams disclosing athlete biometric data to third parties. However, biometric data is typically not categorized as “personal health information” under HIPAA.²⁶ Furthermore, HIPAA guidance explains that professional sports teams are unlikely to fall under the scope of HIPAA.²⁷ Regardless, HIPAA does not address the pertinent issues surrounding athlete ownership or economic rights to biometric data.²⁸

A. State Biometric Laws

In response to the lack of a comprehensive federal data privacy or biometric law, states have taken matters into their own hands by passing laws that regulate the collection and processing of biometric data.²⁹ In 2018, Illinois passed arguably the most impactful and stringent biometric data law in the United States.³⁰

Illinois’ Biometric Information Privacy Act (“BIPA”) differs from other states’ statutes because it requires notice and consent to collect biometric data, regardless of the reason or purpose for the collection.³¹ BIPA strictly prohibits a private entity from selling, leasing, trading, or otherwise profiting from an individual’s biometric data.³² The remainder of states with

²⁵ 15 U.S.C. § 1681 (2012); Pub. L. No. 104-191, 110 Stat. 1936 (1996).

²⁶ Barbara Osborne & Jennie L. Cunningham, *Legal and Ethical Implications of Athletes’ Biometric Data Collection in Professional Sport*, 28 Marq. Sports L. Rev. 37, 47-49 (2017).

²⁷ *Id.*

²⁸ *Id.*

²⁹ *The Evolution of Biometric Data Privacy Laws*, *supra* note 11.

³⁰ Biometric Information Privacy Act, 740 ILCS 14 (2008).

³¹ *Id.* § 15(b)

³² *Id.* § 15(c)

biometric laws only require notice and consent if an individual's biometric identifiers are used for a commercial purpose.³³

Accordingly, while some states have taken the initiative in regulating the collection of biometric data, there is far from a uniform approach to regulating the collection and monetization of biometric data in the United States.³⁴

IV. HOW TO ACHIEVE UNIFORM REGULATION

Because the collection of biometric data deals with personal data, regulation should protect the privacy interests of professional athletes but not go too far so as to prevent athletes from monetizing their biometric data. In order to achieve these goals, uniform proposals should require written notice at or before the collection point, clearly outlining what biometric data is being collected and how that data will be used and monetized. Second, uniform proposals should require informed consent. After having an opportunity to read the written notice explaining how biometric data will be processed and monetized, the athlete should have the opportunity to give or refuse consent. As a result, professional athletes in less centrally regulated sports will be better positioned to negotiate the terms of an agreement and benefit from selling or leasing their biometric data to third parties. With these principles in mind, uniform regulation can be achieved. The crucial question then becomes, who will do the regulating?

A. The Difficulties with Federal or State Biometric Data Regulation

Although a federal and comprehensive data privacy law is likely the most compelling proposal for reaching uniformity, several attempts to pass federal data privacy and biometric laws in the United States have failed.³⁵ Individual states have also failed to pass overlapping

³³ *The Evolution of Biometric Data Privacy Laws*, *supra* note 11.

³⁴ *Id.*

³⁵ Klowsowski, *supra* note 23.

laws, and, further, those that passed such laws have taken different approaches.³⁶ Should states continue to legislate in this area, they should avoid following Illinois' BIPA in creating a blanket prohibition on selling or profiting from biometric data.³⁷ If other states follow Illinois' lead and decide to prohibit the selling or profiting from the general public's biometric data, an exception should be carved out for professional sports athletes when written notice is provided, and the athlete gives informed consent.

In light of the federal and state legislatures' issues with respect to biometric data privacy laws, sports regulatory bodies should be in charge of creating rules regarding the use of athlete biometric data.

B. The Solution: Sports Regulatory Bodies Regulating Athlete Biometric Data

Sports regulatory bodies in less centrally regulated sports should enact rules regulating the collection of athlete biometric data. Self-regulating the collection of biometric data could set a framework for monetizing athlete biometric data in a way that meets high legal and ethical standards. Sports regulatory bodies are best positioned to enact rules regulating biometric data because each sport has different regulatory structures and different commercial uses for biometric data. Further, the development of data privacy laws in the United States is unpredictable.³⁸ Sports regulatory bodies can get ahead of the curve by proactively regulating the monetization of biometric data. By doing so, if or when biometric data laws are enacted, less centrally regulated professional sports will be at the forefront of such regulation. Rather than abusing the lack of uniform laws and preventing athletes from profiting from their biometric

³⁶ *Id.*

³⁷ *See* 740 ILCS 14 § 15(c).

³⁸ *See* Klowsowski, *supra* note 23.

data, sports entities can improve their reputational brand by being transparent and presenting athletes with new revenue streams.

Sports regulatory bodies in less centrally regulated sports should first establish internal policies covering the collection, use, and storage of biometric data. Next, they should focus their efforts on specifying how player data can be collected, whether its collection and use is voluntary, how it will be protected, and how it will be used—ideally, following the principles mentioned above.

More specifically, state athletic commissions that regulate professional boxing and MMA can enact these regulations. For example, the New York State Athletic Commission may authorize a licensed promoter to use an approved data tracking chip or sensor on a combatant’s glove before or during a match in New York State.³⁹ Along with other requirements, the boxing promoter is responsible for notifying both combatants before the match, and the combatants have a right to opt-out without penalty.⁴⁰ The next step would be to create a similar rule that governs the sale or leasing of that data to third parties, including fantasy sports leagues, sportsbook companies, broadcasters, and health and fitness companies.

eSports differs from professional boxing and MMA in that there is no regulatory body that governs the sport. Although that may change in the future, with the Nevada legislature proposing the creation of an eSports commission,⁴¹ self-regulation in eSports will look different than professional boxing and MMA. Instead, eSport leagues should establish internal policies regarding collecting, using, and storing biometric data. Critics may argue that this type of self-

³⁹ *Commission Bulletin 2019-1 Data Tracking Chips*, N.Y. STATE ATHLETIC COMM’N (Jan. 2019), [commission-bulletin-2019-1-data-tracking-chips.pdf](https://www.ny.gov/state-athletic-commission-bulletin-2019-1-data-tracking-chips) (ny.gov).

⁴⁰ *Id.*

⁴¹ Ethan R. Aronson, *Nevada Moves to Create ESports Commission*, NATIONAL LAW REVIEW (Nov. 29, 2021), <https://www.natlawreview.com/article/nevada-moves-to-create-esports-commission>.

regulation has led to the need for more robust data privacy laws in the United States because businesses cannot be trusted to promote data privacy. However, self-regulation will allow the eSports industry to build a strong reputation of trust with athletes, especially when the eSports industry is relatively young and looking to expand.⁴²

CONCLUSION

The monetization of biometric data in professional sports will continue to accelerate as the value of biometric data from wearable devices increases. Biometric data helps athletes improve their performance, decrease injuries, and serves as a potential revenue source through leasing or selling athlete biometric data to third parties like fantasy sports leagues, sportsbook companies, broadcasters, and health and fitness companies.

With the lack of player unions and collective bargaining agreements for athletes in sports like professional boxing, MMA, and eSports, there should be mechanisms to ensure uniform protections, with regulation coming from sports regulating bodies or leagues themselves. This will ensure the athletes are in control of their biometric data and can monetize that data on terms similar throughout their respective sports.

⁴² *The Rise of eSports Investments*, DELOITTE (Apr. 2019), <https://www2.deloitte.com/us/en/pages/advisory/articles/the-rise-of-eSports-investments.html>.