

2021

Should Your Wearables Be Shareable? The Ethics of Wearable Technology in Collegiate Athletics

Sarah M. Brown

Katie M. Brown

Follow this and additional works at: <https://scholarship.law.marquette.edu/sportslaw>



Part of the [Entertainment, Arts, and Sports Law Commons](#)

Repository Citation

Sarah M. Brown and Katie M. Brown, *Should Your Wearables Be Shareable? The Ethics of Wearable Technology in Collegiate Athletics*, 32 Marq. Sports L. Rev. 97 (2022)

Available at: <https://scholarship.law.marquette.edu/sportslaw/vol32/iss1/6>

This Symposium is brought to you for free and open access by the Journals at Marquette Law Scholarly Commons. For more information, please contact megan.obrien@marquette.edu.

SHOULD YOUR WEARABLES BE SHAREABLE? THE ETHICS OF WEARABLE TECHNOLOGY IN COLLEGIATE ATHLETICS

SARAH M. BROWN* & KATIE M. BROWN**

INTRODUCTION

In the era of big data, data collection in sports is booming not only in the form of performance data, but also biometric and real-time positional tracking data. Such data has ushered in the era of a fully “quantified” athlete.¹ Wearable technology (wearables) is a multi-billion-dollar business that has greatly impacted sport competition at all levels. Specifically, professional and amateur organizations, including the National Collegiate Athletic Association (NCAA) utilize wearables, a technology that measures athlete biometric data (ABD) or their physiological measures, like heart rate and body temperature, to gain competitive advantages. Use of wearables has become ubiquitous in NCAA sports, with different teams across all divisions continuously collecting ABD.² Teams can put the ABD into AI-driven video analysis to aid in personnel and strategy decisions and bring in additional revenue.³ Increasing the level of performance is critical for success, and wearables has enabled universities to do just that.

* Dr. Sarah M. Brown is a Clinical Assistant Professor at Southern Methodist University, Dallas, Texas. Dr. Brown earned her PhD from Texas A&M University and her JD from Marquette University Law School. Her research focuses on the marketing and legal aspects of brand management, creation and extension with new technologies and social impact of sport.

** Dr. Katie M. Brown is an Assistant Professor in Sport Management at Texas Tech University, Lubbock, Texas. Dr. Brown earned her PhD from Texas A&M University. Her research focuses on legal issues concerning brand management, intellectual property, and the interfaces of sport marketing, sport law and sport economics.

1. Nick Busca, *As Biometric Boom, Who Owns Athletes' Data Depends on the Sport*, WASH. POST (Feb. 2, 2021, 8:00 am), <https://www.washingtonpost.com/sports/2021/02/02/athletes-biometrics-data-privacy/>.

2. Alicia Jessop & Thomas A. Baker III, *Big Data Bust: Evaluating the Risks of Tracking NCAA Athletes' Biometric Data*, 20 TEX. REV. ENT. & SPORTS L. 81, 87 (2019).

3. *Id.* at 82.

For example, Oregon State University (OSU) has a data and media infrastructure team that is dedicated to providing resources and tools for its athletic department to collect and utilize data.⁴ This team helps the OSU baseball coach understand a pitcher's velocity, performance against left-and-right-handed batters, and even a pitcher's ability to throw strikes during late innings of a game.⁵ Other universities, such as the University of Nebraska, University of Virginia, and William & Mary have embraced wearables to obtain data-driven insights and results are showing that access to this data is having a positive impact on athlete performance.⁶

While data collection has been shown to have a positive impact on team success,⁷ there is also evidence that ABD and collection of such data can be misused or invade on an athlete's privacy. Smart technologies allow for increased surveillance of players that extends well beyond the playing field.⁸ For instance, athletic departments such as Harvard and Penn State University are utilizing WHOOP wearable technology for continuous-monitoring of their athletes, including sleep cycles and fatigue throughout the day.⁹ Additionally, there are already several examples of well-known universities and coaches who blur the line between voluntary and mandatory use of wearables.¹⁰ Further, universities, such as the University of Michigan, have included their athletes' biometric data in sponsorship agreements with companies like NIKE.¹¹

It is evident that universities and even third parties, like NIKE, have an interest in college-athlete biometric data. In fact, data has been collected from college athletes and sold to third parties without bringing college athletes into the conversation.¹² This creates an inherent imbalance of power where decisions are made or potentially forced upon athletes to allow access to intimate personal data. Further, college athletes are not protected by labor laws or collective bargaining agreements, like professional athletes. Thus, the purpose of this article is to discuss the use of wearable technology and ABD in college athletics

4. Chris Hayhurst, *Data Analytics Helps College Coaches and Athletes Optimize Training and Performance*, EDTECH MAG. (Aug. 6, 2019), <https://edtechmagazine.com/higher/article/2019/08/data-analytics-helps-college-coaches-and-athletes-optimize-training-and-performance>.

5. *Id.*

6. *Id.*

7. *Id.*

8. Jessop & Baker, *supra* note 2, at 88.

9. *Id.*

10. Alex Shultz, *Why is This Wearable-Tech Company Helping College Teams Track How Often Athletes Sleep, Drink, and Have Sex?*, DEADSPIN (April 4, 2017, 12:32 PM), <https://deadspin.com/why-is-this-wearable-tech-company-helping-college-teams-1794218363>.

11. Karen Weaver, *Names, Images, Likenesses . . . and Data: Another Issue for NCAA Athletes to Take Seriously*, FORBES (Jan. 1, 2020), <https://www.forbes.com/sites/karenweaver/2020/01/01/names-images-likenessesand-data/?sh=22b67a9a21cc>.

12. Jessop & Baker, *supra* note 2, at 92.

and the resulting power imbalance, explore any rights college athletes have in their ABD, evaluate current laws and policies in place to protect student-athletes, and finally propose a framework that helps protect college athletes' rights without sacrificing the benefits of ABD collection.

I. WEARABLE TECHNOLOGY AND ABD IN COLLEGE ATHLETICS

There are over 400 million wearable smart devices available on the global market.¹³ Wearables are “small electronic and mobile devices or computers with wireless communications capability that are incorporated into gadgets, accessories, or clothes, which can be worn on the human body, or even invasive versions such as micro-chips or smart tattoos.”¹⁴ Despite the prevalence of wearables today, their inception is still very much in its infancy and the industry is expected to grow at more than 20% annually.¹⁵ One of the biggest wearable technologies, with partnerships with the National Football League Players Association (NFLPA), Professional Golf Association (PGA), Major League Baseball (MLB) and most commonly associated with college athletic departments (e.g., Duke University, Penn State University, Harvard and even Conference USA) is WHOOP.¹⁶ WHOOP is a human performance company that offers the WHOOP strap to collect biometric data on strain, sleep, and recovery.¹⁷

Thousands of college athletes wear the WHOOP strap and have their data collected 24/7.¹⁸ The WHOOP Strap 2.0 collects five metrics at 100 times per second; (1) heart rate variability, (2) resting heart rate, (3) body temperature, (4) sleep latency, and (5) skin conductivity—how much you sweat.¹⁹ This data is then uploaded to a computer, providing three daily scores on strain, sleep and recovery to provide individualized insight on how to optimally train and recover. The University of Southern California (USC) is the latest example of a

13. Lionel Sujay Vailshery, *Total Wearable Device Unity Shipments Worldwide 2014-2020*, STATISTA (May 17, 2021),

<https://www.statista.com/statistics/437871/wearables-worldwide-shipments/>.

14. Aleksandr Ometov et al., *A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges*, 193, COMPUT. NETWORKS, 1, 1 (2021).

15. *Id.* at 2.

16. Joe Lemire, *Hey, WHOOP CEO Will Ahmed, What's Next Now That You're a Unicorn?* SPORTTECHIE (Nov. 12, 2020), <https://sporttechie.com/whoop-ceo-will-ahmed-unicorn-funding-athlete-health-fitness-data>.

17. Athletic Medicine, *USC Partners with WHOOP to Maximize Student-Athlete Performance*, USCTROJANS (Apr. 23, 2021), <https://usctrojans.com/news/2021/4/23/athletic-medicine-usc-partners-with-whoop-to-maximize-student-athlete-performance.aspx>.

18. Jackie Williams, *We Need to be Careful When Using Performance Wearables*, MEDIUM (July 30, 2018), <https://medium.com/@JackieWilliams/ever-consider-using-the-whoop-band-things-you-need-to-watch-out-for-c6935ead57b8>.

19. *Id.*

university partnering with WHOOP to maximize their student-athlete's performance.²⁰ The goal is to use the data extracted from the WHOOP strap to give student-athletes a deeper understanding of their bodies and promote general wellness. Currently, 150 USC student-athletes are using WHOOP straps and seeing positive behavioral changes.²¹ Wearables provide a great opportunity for student-athletes to train better, safer, and more effectively. However, the misuse of student-athlete ABD can cause detrimental effects.

In August 2020, it was alleged that then Texas Tech Women's Basketball Head Coach, Marlene Stollings and two assistants, used mandated wearable heart rate monitors in every practice, game, and during workouts to chastise and bully their players.²² It was reported that the first player in the women's basketball locker room on Monday mornings would text a picture of a floor-to-ceiling dry erase board that displayed the results from the wearable heart rate monitors.²³ These results indicated which players had failed to maintain a 90% capacity for more than two minutes during a game.²⁴ This sustained heart rate is higher than the American Heart Association recommends, even for athletes. Such unreasonable and abusive use of wearables and ABD seemingly forced some of the women's basketball players to stop taking over-the-counter painkillers in an effort to use the pain to keep their heart rates spiked.²⁵ While the news of Stollings and her assistants' use of ABD is appalling and there is an underlying fear whether other coaches have similar methods for conditioning their athletes.

Shortly after her dismissal, Stollings filed a lawsuit against Texas Tech University and the athletic director, Kirby Hocutt, claiming breach of contract, fraud, fraudulent inducement, defamation, and sex discrimination.²⁶ The lawsuit argues that Stollings was fired due to "discriminatory biases against female coaches."²⁷ Specifically, the lawsuit said that "Texas Tech and Mr. Hocutt regularly, and in this instance in particular, penalized female coaches for employing the same demanding and effective coaching techniques that male

20. Athletic Medicine, *supra* note 17.

21. *Id.*

22. Jori Epstein & Daniel Libit, *Texas Tech Women's Basketball Players Describe Toxic Culture: 'Fear, Anxiety and Depression'*, USA TODAY SPORTS (Aug. 5, 2020, 3:45 PM), <https://www.usatoday.com/in-depth/sports/ncaaw/big12/2020/08/05/marlene-stollings-texas-tech-program-culture-abuse-players-say/5553370002/>.

23. *Id.*

24. *Id.*

25. *Id.*

26. Madeline Coleman, *Former Texas Tech Women's Basketball Coach Marlene Stollings Files Lawsuit Against School, Athletic Director*, SPORTS ILLUSTRATED (Oct. 21, 2020), <https://www.si.com/college/2020/10/21/texas-tech-womens-marlene-stollings-texas-tech-firing-absue-investigation>.

27. *Id.*

coaches utilize and [have] utilized without consequence.”²⁸ While the lawsuit did not offer specific coaches or universities who may have similar practices, this statement indicates that this type of use of ABD could possibly be used at other universities or with different teams at Texas Tech. There is tremendous pressure on coaches and universities to excel in sports and such pressure can create an environment where coaches are desperate for positive results.

Coercion is a serious concern when it comes to college athletes and their data.²⁹ It was not that long ago (until 2014) when the NCAA used to make every college athlete sign a student-athlete statement where students permitted the sharing of educational records, agreed to drug testing, and waived their publicity rights.³⁰ The NCAA removed student-athletes’ waiver of publicity rights amid lawsuits (e.g., *O’ Bannon v. NCAA*).³¹ Although, until the Supreme Court ruling in *NCAA v. Alston*,³² NCAA bylaws prohibited athletes from being compensated for their name, image and likeness. Now, with the ruling in *Alston*, the Court provided that the NCAA’s prohibition on compensation for college athletes violated Section 1 of the Sherman Act.³³ This ruling, coupled with the name, image and likeness laws passed in various states, gives individual athletes back their right of publicity. Yet, there is the question whether ABD will be considered part of the athlete’s name, image and likeness in which they are able to commercialize. Currently, there is ambiguity around the management of college athlete biometric data, as college athletes sometimes do not have access to their data or understand what data and how often it is being collected.³⁴

The University of Michigan was the first major college brand to consent to collecting private athlete biometric data as part of their apparel contract with NIKE.³⁵ Specifically, the agreement grants NIKE the:

[R]ight to utilize...Activity Based Information...in all media, including, but not limited to, the worldwide web and other interactive and multimedia technologies in connection with the

28. *Id.*

29. Anthony Studnicka, *The Emergence of Wearable Technology and the Legal Implications for Athletes, Teams, Leagues and Other Sports Organizations Across Amateur and Professional Athletics*, 16 DEPAUL J. SPORT L. 195, 197 (2020).

30. John Keilman & Jared S. Hopkins, *College Athletes Routinely Sign Away Rights to be Paid for Names, Images*, CHI. TRIB. (Mar. 26, 2015, 8:23 PM), <https://www.chicagotribune.com/sports/college/ct-ncaa-waivers-met-20150326-story.html>.

31. *Id.*

32. Nat’l Collegiate Athletic Ass’n v. Alston, 141 S. Ct. 2141 (2021).

33. *Id.*

34. Sarah McQuate, *Navigating the Potential Pitfalls of Tracking College Athletes*, UW NEWS (Mar. 2, 2020), <https://www.washington.edu/news/2020/03/02/tracking-college-athletes/>.

35. Weaver, *supra* note 11.

manufacture, advertising, marketing, promotion, and sale of Nike products and Digital Features and programming [which use shall be] on an aggregated, anonymous and de-identified basis and otherwise in compliance with [Big Ten, NCAA, and Michigan] regulations.³⁶

Even though the data is de-identified, it has tremendous value for Nike (e.g., Nike can sell the aggregated data as a product for large amounts of money).³⁷ This is likely why Michigan received \$173 million for a ten year apparel deal.³⁸ At least ten other universities have packaged and sold their athletes' data as part of their sponsorship agreement with NIKE.³⁹ While some of these contracts do have limitations, like University of Nevada Las Vegas requires players to consent and Clemson requires Nike to comply with student and medical privacy laws such as Federal Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA), others do not have parameters on Nike's use of the data.⁴⁰ At this time, Nike is the only apparel company to have rights to harvest athlete data as neither Adidas nor Under Armour have such provisions in their contracts.⁴¹

Universities selling athlete data without their knowledge or consent demonstrates a clear imbalance between the university and its athletes. Athletes' absence from the negotiation table puts them at a grave disadvantage and the potential to miss out on opportunities, opportunities that they may not even be aware of. However, all of this may change with the Alston ruling and the name, image, and likeness laws. Student-athletes may have property rights in their ABD directly related to the right of publicity and trademark rights.⁴² Since ABD is a unique identifier, it will likely be considered part of the athletes' likeness and thus athletes are able to commercialize the data themselves. Thus, presenting a conundrum for universities who have sold their athletes' data without consent.

Further, college student-athletes do not have a union to advocate for specific

36. William Wilson, *Michigan-Nike Contract: The School Seizes and Sells New Player Data*, BOSU (Aug. 31, 2016), <https://brewonsouthu.wordpress.com/2016/08/31/michigan-nike-contract-the-school-seizes-and-sells-new-player-data/>.

37. *Id.*

38. *Id.*

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

40. *Id.*

41. *Id.*

42. Kristy Gale, *The Sports Industry's New Power Play: Athlete Biometric Data Domination. Who Owns It and What May be Done with It*, 6 ARIZ. ST. U. SPORTS & ENT. L. J. 7, 19 (2016).

standards concerning wearable use or the management of ABD. College athletes are not protected by labor laws or collective bargaining agreements. Therefore, the only policy protections afforded to athletes are those at the university level and NCAA level. In 2015, the NCAA Committee on Competitive Safeguards and Medical Aspects of Sports discussed wearable technology and its place in college sport. Out of this discussion the committee made four recommendations:

- (1) The data generated by those technologies should be used in conjunction with the sports medicine team to ensure health and safety are taken into account.
- (2) No matter what the data indicates, athletics health care providers should have unchallengeable autonomous authority to determine medical management and make return-to-play decisions.
- (3) The NCAA Playing Rules Oversight Panel should consider changing relevant playing rules to ensure that they facilitate the implementation of the new technologies.
- (4) Those permissive modifications should not run afoul of existing playing equipment standards, certifications and warranties.⁴³

This meeting was held over six years ago and the NCAA is still lagging behind in their protections for student-athletes' biometric data.

Currently, the NCAA does not offer an overarching policy for the use of wearables or management of ABD. Rather, the NCAA has approached its sports individually as far as developing a plan for wearable technology. The NCAA allows the use of wearables in games; however, it prohibits real-time data analysis during games to the extent such analysis is used to make performance enhancing adjustments.⁴⁴ The NCAA does not offer guidance on the use of wearables during practice or how that data should be protected and managed. For example, the NCAA released new rules around wearables in the 2019-2020 and 2020-2021 swimming and diving rulebook. The new rule said:

[t]he use of technology and automated data collection devices

43. Chris Radford, *Competitive Safeguards Committee Supports SEC Concussion Proposal, Wearable Technology Use*, NCAA (Jan. 15, 2015), <https://www.ncaa.org/about/resources/media-center/news/competitive-safeguards-committee-supports-sec-concussion-proposal-wearable-technology-use>.

44. Robyn Feldstein et al., *Wearables in the Arena: The Shifting Legal Landscape Governing Fitness Trackers in Professional Sports*, JDSUPRA (Dec. 18, 2018), <https://www.jdsupra.com/post/contentViewerEmbed.aspx?fid=a45573cd-ffea-48da-9f3d-dff7c9e34363>.

is permissible for the sole purpose of collecting data. Automated devices shall not be utilized to transmit data, sounds or signals to the athlete and may not be utilized to effect pace or tempo. The device(s) may be worn in any fashion, including on the wrist.⁴⁵

These sparse guidelines and policies fall short of the protections college athletes deserve. The data collected is extremely private and, as evidenced by the multi-million-dollar contracts, is immensely valuable. Such a commodity needs to be afforded safeguards to ensure college athletes are not exploited, either intentionally or unintentionally. Before appropriate protections can be put in place, it is essential to understand the rights athletes have within their data.

II. COLLEGE ATHLETE'S RIGHTS AND PROTECTIONS FOR ABD COLLECTION

Despite being amateur athletes, college athletes have the right of publicity and the right of privacy in their ABD. Additionally, student-athletes may have some protection under FERPA. While athletes may have these rights, it is critical to note that they are not absolute and, in some situations, can be waived by the athlete. Below is a review of the right of privacy, the right of publicity and FERPA and their application to college athletes' ABD.

A. College Athlete's Right of Privacy in their ABD

With the explosion of wearables and the increased collection of biometric data, states have increasingly been working towards creating privacy laws or specific biometric laws. This right is rooted in common law and its guidelines vary state-by-state. However, the crux of privacy laws is to secure "each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."⁴⁶ The right of privacy is equally afforded to any expression and the right is only lost when the individual publicizes the information himself.⁴⁷ Thus, privacy laws are aimed at securing individuals the right to provide information to the public as they see fit.⁴⁸

Currently, the most comprehensive state privacy law is the California Consumer Privacy Act (CCPA), which was signed into law in June 2018 and

45. Greg Lockard, *NCAA Swimming and Diving Rules Book*, NAT'L COLLEGIATE ATHLETIC ASS'N (2019), <https://www.ncaapublications.com/productdownloads/SW20.pdf>.

46. Samuel D. Warren & Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193, 199 (1890-1891).

47. *Id.*

48. *Id.*

went into effect January 2020.⁴⁹ The purpose of the CCPA is to give consumers control over their personal information that businesses collect about them. Specifically, the law secures new privacy rights for California residents, including:

- (1) The right to know about the personal information a business collects about them and how it is used and shared;
- (2) The right to delete personal information collected from them (with some exceptions);
- (3) The right to opt-out of the sale of their personal information; and
- (4) The right to non-discrimination for exercising their CCPA rights.⁵⁰

Personal information under the act includes any information that identifies, relates to, or could reasonably be linked with an individual or their household.⁵¹ Although, the Act does not explicitly state biometric data, biometric data is an identifier and would likely fall within the protection of the CCPA. Another important component of the CCPA is that the privacy right cannot be waived.⁵² A waiver has traditionally been an easy mechanism for businesses to comply with these types of regulations more easily. The CCPA applies to all businesses (even those outside of California) that: (1) have a gross annual revenue of over \$25 million, (2) buy, receive, or sell the personal information of 50,000 or more California residents, households or devise; or (3) derive 50% or more of their annual revenue from selling California residents' personal information.⁵³ While CCPA does not directly apply to most universities and colleges because of their nonprofit status, it could apply to any third party vendors the universities use to collect their athletes data (e.g., WHOOP and Nike).⁵⁴ The CCPA was recently updated by the California Privacy Rights Act in November 2020, which enhanced consumer protections and includes biometric information. These

49. Angelique Carson, *Data Privacy Laws: What You Need to Know in 2021*, OSANO (July 20, 2021), <https://www.osano.com/articles/data-privacy-laws#:~:text=There%20is%20no%20one%20comprehensive,information%2C%20financial%20institutions%20and%20marketing.>

50. Cal. Civ. Code §§1798.100-1798.199 (West 2018).

51. *Id.*

52. *Id.*

53. *Id.*

54. Joshua Metayer, *What Does the CCPA Mean for Colleges and Universities*, INT'L ASS'N OF PRIVACY PROF. (March 26, 2019), <https://iapp.org/news/a/what-does-the-ccpa-mean-for-colleges-and-universities/>.

amendments will go into effect in January 2023.⁵⁵

New York is another state that has broad legislation giving greater protection to privacy rights. The Stop Hacks and Improve Electronic Data Security (SHIELD) Act, amended the existing data breach notification law and imposed more data security requirements on organizations collecting data from New York residents.⁵⁶ The SHIELD Act introduces significant changes, including: (1) broadens the definition of private information to include biometric information, (2) expands the definition of breach from *unauthorized acquisition* to *unauthorized access*, (3) expands the territorial scope to any person or business that collects data from a New York resident, and (4) imposes specific data security requirements.⁵⁷ The SHIELD Act and the CCPA share similarities in their scope and currently are the most robust effective privacy laws. Both Virginia and Colorado have passed statutes that afford their residents similar protections to the CCPA and the SHIELD Act, but do not go into effect until January 1, 2023.⁵⁸

The right of privacy has been litigated in the sport context, specifically whether athletes have a diminished expectation of privacy as a result of their participation in sport, at the federal level.⁵⁹ Specifically, the Fourth Amendment of the Constitution gives every citizen the “right to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”⁶⁰ While college athletes will likely not utilize the Fourth Amendment to protect their rights with their ABD, it is still important to understand the possible implication of the Fourth Amendment. While college athletes may have a state law right of privacy in their ABD, they can be compelled to share their ABD as part of a search warrant.⁶¹ Thus, college-athletes need to be aware that all of the data being collected, including GPS tracking, can be legally seized. While some privacy laws can help protect athletes’ interests, others may be harmful to an athletes’ interest. This demonstrates the importance of athletes understanding what data is being collected.

55. Carson, *supra* note 49.

56. S. B. S5575B, 1st Sess. (N.Y. 2019-2020).

57. *Id.*

58. Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-580 (2021); Colorado Privacy Act, COLO. REV. STAT. § 6-1-1301 (2021).

59. *See, e.g.*, student-athletes constitutional right of privacy diminished in Vernonia School Dist. 47J v. Acton, 515 U.S. 646 (1995) (where the Court held that a public school could require random urine drug testing for students who participate in athletic programs); Joy v. Penn-Harris-Madison Sch. Corp., 212 F.3d 1052, 1059 (7th Cir. 2000) (the court said, “students who voluntarily participate in school athletics have reason to expect intrusions upon normal rights and privileges, including privacy.”).

60. U.S. Const. amend. IV.

61. *In Re* Search Warrant No. 5165, 470 F. Supp. 3d 715 (E.D. Ky. 2020).

B. Biometric Laws

Although privacy laws can be applied to biometric data, recently there has been increased lobbying for specific biometric laws.⁶² Presently, there are five states with existing biometric specific laws and multiple others have proposed biometric laws.⁶³ Illinois, Biometric Information Privacy Act (BIPA) enacted in 2008 is the oldest and most expansive biometric specific law.⁶⁴ BIPA has five key features:

- (1) Requires informed consent prior to collection
- (2) Permits a limited right to disclosure
- (3) Mandates protection obligations and retention guidelines
- (4) Prohibits profiting from biometric data
- (5) Creates a private right of action for individuals harmed by BIPA violations
- (6) Provides statutory damages up to \$1,000 for each negligent violation, and up to \$5,000 for each intentional or reckless violation.⁶⁵

This law ensures that individuals are in control of their biometric data and greatly restricts companies from collecting data unless they: (1) inform the person in writing of the data collected or stored, (2) inform the person in writing the specific purpose and length of time the data will be collected, stored and used, and (3) obtain consent.⁶⁶ BIPA went largely unnoticed until 2015 when there was a series of class action lawsuits against businesses alleging unlawful collection and use of biometric data of Illinois residents.⁶⁷ More lawsuits continued to follow as the bounds of BIPA were tested. The most recent significant decision came in January 2019 when the Illinois Supreme Court held in *Rosenbach v. Six Flags*⁶⁸ that actual harm is not a requirement to establish

62. Amy De La Lama, Lauren J. Caisman, and Melissa R. Whigham, *United States: U.S. Biometric Laws & Pending Legislation Tracker*, MONDAQ (May 18, 2021), <https://www.mondaq.com/unitedstates/privacy-protection/1068486/us-biometric-laws-pending-legislation-tracker#:~:text=Also%20prohibits%20a%20person%20in,by%20the%20Texas%20Attorney%20General.>

63. *Id.*

64. 740 ILL. COMP. STAT. 14/1 (2008).

65. *See id.*

66. *Id.*

67. *See Patel v. Facebook Inc.*, No. 1:15-cv-04265 (N.D. Ill. 2015) (Facebook was ordered to pay a \$650 million settlement for beaching BIPA by using facial tagging features without the consent of Illinois residents).

68. *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197 (Ill. 2019).

standing to sue under BIPA. This landmark decision will likely open the floodgates for future litigation surrounding biometric data. However, the definition of biometric identifier in BIPA is limited to “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry” and expressly excludes biological samples, physical descriptors, medical images, and photographs.⁶⁹ This means that BIPA likely does not extend its protections to ABD. Yet, with the surge in biometric and privacy laws, it is possible for Illinois to update the definition of biometric identifier to include physiological measures.

Texas was the next state to enact Capture or Use of Biometric Identifier (CUBI) in 2009.⁷⁰ Similarly, to BIPA, Texas narrowly defines biometric identifiers as eye scans, fingerprints, voiceprints and hand or face geometry.⁷¹ The law prohibits the collection and sale of these identifiers without first providing information to the data subjects and receiving their consent, but such consent does not need to be written.⁷² Additionally, CUBI requires that businesses destroy any biometric data that is no longer needed within a reasonable time, but not longer than one year.⁷³ This law differs from BIPA in that it does not provide a private right of action.⁷⁴ Since the definition of biometric identifier is limited under CUBI, it likely will not apply to ABD. Yet, that could all change in the near future.

Next, Washington enacted a biometric privacy law, HB 1493, in 2017.⁷⁵ This law, like BIPA and CUBI, sets forth requirements for businesses who collect and use biometric identifiers for commercial purposes.⁷⁶ Unlike, BIPA and CUBI, this law defines biometric identifier as a measurement of an individuals’ biological characteristics, thus collection of ABD would likely fall within this law.⁷⁷ HB 1493 focuses on individuals who have enrolled into a biometric identifier database.⁷⁸ Further, HB 1493 does not explicitly provide how consumers must be given notice or consent obtained. Rather the law leaves this decision as “context-dependent.”⁷⁹ Like CUBI, HB1493 does not provide a private right of action, its enforcement is dependent on the Washington Attorney

69. 740 ILL. COMP. STAT. 14/10 (2008).

70. TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021).

71. TEX. BUS. & COM. CODE ANN. § 503.001(a) (West 2021).

72. TEX. BUS. & COM. CODE ANN. § 503.001(c)(1) (West 2021).

73. TEX. BUS. & COM. CODE ANN. § 503.001(c)(3) (West 2021).

74. TEX. BUS. & COM. CODE ANN. § 503.001(d) (West 2021).

75. WASH. REV. CODE ANN. § 19.375.020 (West 2021).

76. *Id.*

77. WASH. REV. CODE ANN. § 19.375.010 (West 2021).

78. *Id.*

79. WASH. REV. CODE ANN. § 19.375.020 (West 2021).

General.⁸⁰

With the recent surge of biometric data collection, states have increasingly expanded their existing privacy laws to include biometric data or states have been more active at creating biometric laws. For example, New York has recently added a biometric regulation to their administrative code. New York City's Administrative Code, Biometric Identifier Information⁸¹ is more inclusive in its definition and defines biometric information as a physiological or biological characteristic.⁸² This regulation requires that any establishment that collects, retains, converts, stores or shares biometric information must disclose such use with a clear and conspicuous sign near all entrances of the establishment.⁸³ The regulation further prohibits the commercialization of any collected biometric data.⁸⁴ Lastly, this regulation, like BIPA, allows for a private right of action.⁸⁵

It is evident that there is concern for the management of biometric information. This concern will only continue to go as wearable and smart technology continues to advance procuring even more invasive data. Further, there is still an uncertain legal status of ABD and how it would be treated under these laws. However, with the ruling in *Alston*, and student-athletes' ability to profit from their name, image, and likeness, we will likely see future cases on the protections of ABD.

C. College Athlete's Right of Publicity in Their ABD

The right of publicity is an intellectual property right and was first acknowledged in American common law in the 1950s.⁸⁶ The right of publicity became a statutory right in California in 1972⁸⁷ and recognized by the U.S. Supreme Court in 1977.⁸⁸ Currently, the right of publicity is established by either statute or common law in 35 states.⁸⁹ This right gives individuals the

80. *See id.*

81. 12 N.Y.C. ADMIN. CODE § 22-1201.

82. *Id.*

83. Biometric Identifier Information, § 22-1202.

84. *Id.*

85. Biometric Identifier Information, § 22-1203.

86. *See Haelan Labs, Inc. v. Topps Chewing Gum, Inc.*, 202 F.2d 866 (2d Cir. 1963).

87. CAL. CIV. CODE §§ 3344–3344.1 (West 2021).

88. *Zacchini v. Scripps-Howard Broad. Co.*, 433 U.S. 562, 564-65 (1977).

89. As of 2020, the following states recognizing the right of publicity: Alabama (ALA. CODE § 6-5-770), Arizona (ARIZ. REV. STAT. ANN. § 12-761 (2007) (applies only to soldiers)), Arkansas (ARK. CODE ANN. § 4-75-1101 (2016)), California (CAL. CIV. CODE § 3344), Colorado (*Donchez v. Coors Brewing Co.*, 392 F.3d 1211 (10th Cir. 2004)), Connecticut (*In re Jackson*, 972 F.3d 25 (2d Cir. 2020)), Florida (FLA. STAT. § 540.08 (2007)), Georgia (*Bullard v. MRA Holding, LLC*, 740 S.E.2d 622 (Ga.

control to commercialize their identity.

The right of publicity has been an evolving legal landscape for college athletes. Up until the recent ruling in *NCAA v. Alston*, college athletes were restricted from profiting from their name, image, and likeness (NIL). As noted earlier, college athletes were obligated to waive their right of publicity and allow both their university and the NCAA to profit from their name, image, and likeness. While the NCAA still has some restrictions on the commercialization of athletes' name, image, and likeness, including:

- (1) No use of NCAA intellectual property . . . from colleges or conferences in endorsements;
- (2) Colleges and Conferences cannot make payments for endorsements;
- (3) Colleges and Conferences cannot arrange endorsement deals for Student-Athletes;
- (4) Colleges and Conferences cannot use endorsements or allow boosters to use endorsements, in a way which could be considered pay for play;
- (5) Colleges and Conferences cannot use endorsements for recruiting by schools or boosters; and
- (6) Agents and advisors will be regulated.⁹⁰

Student-athletes have reclaimed their right of publicity. Given the novelty

2013)), Hawaii (HAW. REV. STAT. § 482P-1 (2009)), Illinois (765 ILL. COMP. STAT. 1075/1), Indiana (IND. CODE § 32-36-1-1 (2012)), Kentucky (KY. REV. STAT. ANN. § 391.170 (2020)), Massachusetts (MASS. GEN. LAWS ch. 214, § 3A (2020)), Michigan (Hauf v. Life Extension Found., 547 F. Supp. 2d 771 (W.D. Mich. 2008)), Minnesota (Ventura v. Titan Sports, Inc., 65 F.3d 725 (8th Cir. 1995)), Missouri (Doe v. TCI Cablevision, 110 S.W.3d 363 (Mo. 2003)), Nebraska (NEB. REV. STAT. § 20-201 (2020)), Nevada (NEV. REV. STAT. § 597.770), New Hampshire (Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288 (D.N.H. 2008)), New Jersey (Estate of Presley v. Russen, 513 F. Supp. 1339 (D.N.J. 1981)), New Mexico (Moore v. Sun Publ'g Corp., 881 P.2d 735 (N.M. Ct. App. 1994)), New York (N.Y. CIV. RIGHTS LAW §§ 50–51 (applies only to living individuals) (2020)), Ohio (OHIO REV. CODE ANN. § 2741.01 (2002)), Oklahoma (OKLA. STAT. tit. 21, § 839.1 (2020)), Pennsylvania (42 PA. CONS. STAT. § 8316 (2003)), Rhode Island (9 R.I. GEN. LAWS § 9-1-28.1 (2016)), South Carolina (Gignilliat v. Gignilliat, Savitz & Bettis, L.L.P., 684 S.E.2d 756 (S.C. 2009)), South Dakota (S.D. CODIFIED LAWS § 21-64-2 (2015)), Tennessee (TENN. CODE ANN. § 47-25-1101 (2020)), Texas (TEX. PROP. CODE ANN. § 26.001 (1987)), Utah (UTAH CODE ANN. § 45-3-1 (1981)), Virginia (VA. CODE ANN. § 8.01-40 (2015)), Washington (WASH. REV. CODE § 63.60.010 (2008)), West Virginia (Crump v. Beckley Newspapers, Inc., 320 S.E.2d 70 (W. Va. 1983)), and Wisconsin (Hirsch v. S.C. Johnson & Son, Inc., 280 N.W.2d 129 (Wis. 1979)).

90. Intellectual Property Center, *NCAA Allows Right of Publicity Endorsement*, THEIPCENTER.COM (April 29, 2020), <https://theipcenter.com/2020/04/student-athletes-earning-money-from-rights-of-publicity>.

of the ruling in *Alston* and the NIL laws, there has not been much clarity on where ABD will fall. An individual's NIL includes unique identifiers, such as an athlete's biometric data, however, ownership of the data is ambiguous. The problem becomes even more concerning because athletes may not be fully informed on what data is being collected and how it is being used. However, since ABD is a unique characteristic identifier and likely considered part of the athlete's ABD, it is probable that they can commercialize their ABD to some extent under the new NCAA policy and state laws.

The NIKE endorsement deals (e.g., University of Michigan) are examples of how student-athlete biometric data can be packaged and sold.⁹¹ However, NCAA rules clearly state that a college or conference cannot pay an athlete for endorsements, therefore athletes are unlikely to profit from these types of endorsement deals between apparel manufacturers and the university. Yet, what is to stop an athlete from selling their personal data to a third party under an endorsement deal? Currently, unclear ownership is the major barrier to athletes utilizing ABD as a commercialized commodity. Student-athletes could argue that they own the data because it is their personal information. However, universities could claim that they own the data because they have paid for the wearable devices to improve the student-athlete's performance and increase their safety while they are an athlete at the university. The university could also posit that by the student-athlete voluntarily using the wearable or smart technology, they are relinquishing ownership to the university to use the data. The crux of college athlete ABD ownership comes down to student-athletes being informed.

Athlete publicity and data ownership rights have been litigated across the country with courts' opinions on who has interests in team names, athlete likeness, statistics and data.⁹² Indiana, a state that affords broad protections to publicity rights, has produced the most recent ruling in this area in *Daniels v. FanDuel*.⁹³ In this case, the plaintiffs, Akeem Daniels and two other former college football players alleged that the defendants violated Indiana's right of publicity statute by displaying the plaintiffs on their fantasy sports sites.⁹⁴ The Indiana right of publicity defines a person's right of publicity as "a person's property interest in the personality's: (1) name, (2) voice, (3) signature, (4) photograph, (5) image, (6) likeness, (7) distinctive appearance, (8) gestures, (9) mannerisms."⁹⁵ However, the statute does provide four exceptions; (1) when the

91. Weaver, *supra*, note 11.

92. Irwin Raj, *Murphy and Athletes' Publicity Rights*, OMM.COM (Oct. 31, 2018), <https://www.omm.com/resources/alerts-and-publications/alerts/murphy-and-athletes-publicity-rights/>.

93. *Daniels v. FanDuel, Inc.*, 109 N.E.3d 390, 392 (Ind. 2018).

94. *Id.* See IND. CODE § 32-36-1-8(a) (2019).

95. *Daniels v. FanDuel, Inc.*, No. 1:16-cv-01230-TWP-DKL, 2017 U.S. Dist. LEXIS 162563, at *2 (S.D. Ind. Sept. 29, 2017).

content is newsworthy, (2) when the content is of general or public interest, (3) used in literary works, and (4) truthfully identified the actual performer.⁹⁶ In their ruling, the district court utilized the “newsworthy” and “public interest” exceptions to evaluate whether they could be applied to a commercial venture in the use of players names for fantasy football. The court first relied heavily on common law rulings to define “newsworthy” and eventually determined that plaintiff’s athletic achievements and activities were newsworthy.⁹⁷ Next, the district court focused on whether players’ names were of “public interest.” The exception conditions the public interest on the broadcasting or reporting of an event. The court distinguished this case from other similar cases regarding the use of players as avatars in video games, noting that fantasy sport websites are used for fans to gather information. Further, all of the information provided on the websites was already available to the general public.⁹⁸ Following the district court’s ruling, the plaintiffs appealed to the U.S. Court of Appeals for the Seventh Circuit. The appellant court did not want to address the issue of application of the statutory exemptions and instead certified the question to the Indiana Supreme Court. The Indiana Supreme Court unanimously rejected the plaintiff’s right of publicity claim, concluding that the use of statistical information was protected under the “newsworthy” exception.⁹⁹ In this ruling the Indiana Supreme Court opined that the term “newsworthy” was understood to encompass a broad privilege that was “defined in the most liberal and far-reaching terms.”¹⁰⁰

This precedent is concerning in terms of protection of college athletes’ right of publicity, particularly rights stemming from their ABD. The Indiana Supreme Court said statistical information was protected under the newsworthy exception, but it did not put any limitations on types of statistical data. The scope of information found in statistics has vastly increased with wearables, including biometric measures.¹⁰¹ So, does this mean that the protections afforded to third parties in *Daniels* would also be afforded in any rights of publicity case around athlete ABD? The lines are certainly blurry when you consider the diminished expectation of privacy of athletes and the likely public interest and underpinning newsworthiness of fans having access to ABD.

96. IND. CODE § 32-36-1-1(c)(1)(B) (2019).

97. *Daniels*, 2017 U.S. Dist. LEXIS 162563, at *16-18.

98. *Id.*, at *24.

99. *Daniels v. FanDuel, Inc.*, 109 N.E.3d 390, 393, 396 (Ind. 2018), *aff’d*, 909 F.3d 876 (7th Cir. 2018).

100. *Daniels*, 109 N.E.3d at 395.

101. Mark Conrad, *A new Standard for Right of Publicity Protection for Statistics in the Era of Daily Fantasy Sports and Legalized Sports Betting—A Critique of Daniels v. FanDuel and a Revival of an Economic-Based Rationale to Protect Athletes’ Property Rights*, 38 CARDOZO ARTS & ENT. L.J. 1, 30 (2020).

D. FERPA and ABD

College athletes may seek protection for their ABD under FERPA.¹⁰² FERPA applies to all schools that received funds under an applicable program of the U.S. Department of Education. Under FERPA generally, schools must have written permission from the parent or eligible student in order to release any information from a student's record.¹⁰³ A student's record contains personally identifiable information, which includes a student's biometric record.¹⁰⁴ A biometric record means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. While on its face the definition of biometric record does not seem inclusive of ABD, it could be modified and extended to further protect student-athletes. A modification that is possible if wearable technology continues to permeate college athletics.

However, even if ABD was protected under the current version of FERPA or modified to be included, student-athletes must sign a FERPA waiver for the NCAA to review educational documents.¹⁰⁵ Despite the waiver being limited, it does allow for the university to share personally identifiable information with the NCAA and the university's conference.¹⁰⁶ Therefore, college athletes may not be able to restrict the disclosure of their ABD from the university to the NCAA, but if the FERPA language is modified to include ABD this would restrict universities from packaging and selling the data to third parties like NIKE. Thus, Michigan's agreement with NIKE would be in violation of FERPA.

III. PROPOSED FRAMEWORK TO PROTECT STUDENT-ATHLETES

Protection of a student-athlete's interest in their biometric data is multi-layered, as there are various concerns. A potential framework for managing student-athlete ABD should include three main considerations. First, there needs to be clear guidelines and limitations on athlete consent for collection and use of ABD. Second, there needs to be protection against potential misuse of the data. Third, consideration should be given to whether student-athletes can commercialize their data independently under the new NIL policy and state laws. For adequate protection, each concern must be addressed individually.

102. 20 U.S.C. § 1232g; *See* Family Educational Rights and Privacy, 34 C.F.R. § 99 (2021).

103. 34 C.F.R. § 99 (2021).

104. 34 C.F.R. § 99.3 (2021).

105. Michael Bragg, *FERPA Defense Play: Universities Often Cite the Federal Student Privacy Law to Shield Athletic Scandals*, STUDENT PRESS LAW CTR., (March 31, 2015), <https://splc.org/2015/03/ferpa-defense-play/>.

106. NCAA, *Form 21-1a: Student-Athlete Statement*, (2021).

First and foremost, there needs to be clear communication on what it means for a student-athlete to consent to the collection of their biometric data. This means each university should provide in writing to its athletes exactly what data they are planning to collect, the purpose for the collection, what personnel will have access to the data, and how that data will be used. These requirements mirror those found in the CCPA and provide clarity on what it means and what can happen if the athlete consents to collection of ABD. Another pivotal component to consent is that it should not be contingent on their ability to participate in the sport. By making consent a prerequisite to participation, the university is indirectly influencing the voluntariness of consent. Lastly, if a student-athlete does give consent to have their ABD collected, there needs to be limitations on that consent to avoid misappropriation and abuse. These limitations can be outlined and explained in the consent document that describes the purpose and use for ABD collection. This language should be specific and inclusive.

Second major concern to address is how ABD is being used by universities. As previously discussed, athletes' biometric data has been used in an abusive manner (e.g., Texas Tech Women's basketball coach Marlene Stollings). Clear guidelines from the NCAA need to be written that outline and prohibit such uses of ABD. This is an issue to be handled at the NCAA level because there needs to be standardization among all universities. Further, the NCAA is able to levy severe penalties to universities who do not follow the guidelines. The NCAA has already formed a committee dedicated to athlete biometrics that is composed of attorneys, athletes and academics. This committee would be ideal for creating such guidelines to protect student-athletes from ABD misuse.

Also under this second concern is the misappropriation of student-athlete data. Misappropriation occurs when the student-athletes' data has been used in violation of their right of privacy, right of publicity or in contravene of the uses the athlete consented too. While an athlete could sue for misappropriation of ABD under the right of privacy and right of publicity there is ambiguity, due to lack of precedent, in how courts would handle the matter. Thus, there is value in creating a specific federal law targeting athlete biometric data. While there is not a federal law protecting individuals' right of publicity or right of privacy, there has been increased lobbying for such laws. Further, the NCAA has asked Congress to make a uniform federal law to manage student-athletes' rights to profit from their name, image, and likeness while in college. It seems appropriate that Congress should also address ABD with federal legislation.

The third concern is about student-athletes' ability to commercialize their own data. There is certainly going to be opportunity and demand for athlete data. Evidence of this is seen in the multiple agreements that NIKE has with universities to collect and utilize the athletes' data for a variety of purposes. For students to commercialize their data, they need to have clear ownership of data.

While athletes likely have de facto ownership of the data since they need to give consent to collection, it still needs to be explicitly stated that athletes will own and have access to any data collected. Student-athletes should have the opportunity to sell that data to a third-party under the new NIL laws and policy. This is a financial opportunity that should be restricted to the student-athlete only. However, a student-athlete needs to fully understand that by selling their data to a third party means that the data could become publicly available, depending on the terms of the agreement, and negative consequences could result. For example, a student-athlete could sell their data to a gambling company, such as FanDuel, and if the data indicates underlying issues with the athlete, they will not be able to use right of privacy to protect themselves. There may be good opportunities for student-athletes to generate revenue, but they need to be aware of potential repercussions. Lastly, it should be left to the athlete on whether they want to commercialize their data, otherwise the NCAA may find itself in a similar situation that it did in *O'Bannon v NCAA*.

CONCLUSION

The collection of ABD in college athletics has been thrust to the forefront of national conversation, as more universities implement wearables into their athlete training programs. Evidence shows that access to wearables and ABD can provide a competitive advantage, but also create a situation of susceptibility of data misuse, resulting in abuse of student-athletes. Largely, there are minimal guidelines on the management of wearables and ABD in college athletics, creating potential problems for student-athletes. Further, sparse legal precedent regarding ABD creates much ambiguity around the potential protections afforded to college athlete's ABD. Lastly, college athletes' recent victory in *NCAA v. Alston*, enables them to profit from their NIL, a right previously waived. With this new precedent there may be an opportunity to monetize their ABD, as demand and desire for the data has been established with multiple universities making deals with third parties to package and sell its athletes' ABD.

After evaluating current use of ABD in college athletics, privacy laws, biometric laws, right of publicity laws, and application of FERPA to ABD it was determined that new protections need to be put in place to protect student-athletes' interests. Specifically, three main areas were identified, (1) clear guidelines and limitations on athlete consent and use of ABD, (2) regulations on use of ABD and associated penalty for misuse, and (3) allow student athletes to determine whether they want to commercialize their ABD.

The collection of ABD has become routine in college athletics to the point where some student-athletes are not aware of what data is being collected and how it is being used. There should not be an expectation of athletes to

automatically provide should personal data to their university. Rather student-athletes need to be informed so they are empowered to make an educated decision about the management and use of their ABD.