Access Denied: Banning the Monetization of Student-Athlete Biometric Data in College Sports

DAIRANETTA S. SPAIN*

---

* Staff Member, Volume 50, and Managing Editor, Volume 51, *The University of Memphis Law Review*; Juris Doctor Candidate, The University of Memphis Cecil C. Humphreys School of Law, 2021. In memory of my loving brother, Tony. I am forever grateful to Professor Lynda Wray Black for championing my ideas and providing invaluable guidance throughout the Note process. Special thanks to: Kayla Billingsley, my Notes Editor, who dove deep into the world of biometric privacy to offer helpful guidance in developing my Note; Becca Payton and Louis Bernsen for stellar assistance during the editing process; my parents, family, friends, professors, and mentors, thank you for continuing to be a solid, unwavering support system; and finally my darling son, Micah, my greatest source of inspiration.

I. INTRODUCTION

Nineteen-year-old Asia Cummings wakes up each morning at 4:00 a.m. for mandatory track and field workouts, which may include morning runs or weight training. Her typical day includes breakfast, followed by classes, and a two-hour track practice. Asia has struggled with ailing shin splints for years, which often develop into stress fractures due to insufficient arch support. To combat this reoccurring injury, trainers and team doctors monitor Asia's stress and arch pressure through an electronic chip installed in her shoe. The data metrics allow team trainers and doctors to recommend intermittent breaks—and even complete rest—when her numbers predict a shin splint is inevitable. As a general practice within college sports, this information and the supporting algorithms are routinely shared across college sports between athletic trainers and coaches to prevent agonizing injuries, such as stress fractures, from plaguing the developing body of the average student-athlete.

Asia's story is fictitious. However, Asia's story is representative of the current practice of monitoring student-athlete biometric data among college sports for the purposes of assessing athletic activity, stress, sleep, and other performance-related data points.[1] While student-athlete biometric data ("ABD") can be leveraged for the good of the student-athlete's developing body, use of the information accessed through a wearable tracking device ("wearable"), like the chip worn in Asia's shoe, is not always limited to performance and health benefits. Leading marketers project the wearables market to surpass $27 billion by 2022.[2] Many companies may capitalize on device sales to individual consumers,[3] and sporting apparel companies gain to realize profits by leveraging metrics obtained through ABD monitoring.

In fact, Nike has taken advantage of harvesting student-athlete biometric data through strategic partnerships with NCAA institutions granting the right to acquire the data. In 2016, Nike and the University of Michigan entered a $170 million sponsorship deal.[4] This deal turned heads and raised privacy concerns because a particular clause granted Nike a contractual right to collect ABD.[5] The deal was purportedly a part of Nike's efforts to enhance its ability to collect performance data from student-athletes.[6] Nike's reach extended further—at least eleven

---

1. *See* discussion *infra* Section II.C. Wearable tracking devices are the most common method by which ABD is collected among college sports.

2. Paul Lamkin, *Smart Wearables Market to Double by 2022: $27 Billion Industry Forecast*, FORBES (Oct. 23, 2018, 8:04 AM), https://www.forbes.com/sites/paullamkin/2018/10/23/smart-wearables-market-to-double-by-2022-27-billion-industry-forecast/#27c87bad2656.

3. *Id.*

4. Marc Tracy, *With Wearable Tech Deals, New Player Data Is Up for Grabs*, N.Y. TIMES (Sept. 9, 2016), https://www.nytimes.com/2016/09/11/sports/ncaafootball/wearable-technology-nike-privacy-college-football.html.

5. Mathew Kish, *Nike's Expanded Effort to Collect Data from College Athletes Raises Privacy Concerns*, PORTLAND BUS. J. (Sept. 15, 2016, 2:57 PM), https://www.bizjournals.com/portland/news/2016/09/15/nikes-expanded-effort-to-collect-data-from-college.html.

6. *Id.*

other schools with similar contractual deals provided Nike player data through wearables at the time.[7]

Student-athlete biometric data should be leveraged primarily for the good of student-athletes and not for economic gain among the National Collegiate Athletic Association ("NCAA") member institutions and third-party vendors. The solution presented here bars the monetization of such personal data absent meaningful consent and realizes an endorsement opportunity for student-athletes in an age where growing momentum presents an opportunity for student-athletes to profit from their names, images, and likenesses ("NIL") further chipping away at the NCAA traditional amateurism model. This Note proposes a state legislative and regulatory framework that bans the NCAA, its institutions, and third parties from monetizing student-athlete biometric data without meaningful consent. Currently, a gap exists in regulating student-athlete biometric data, and the use of the data implicates rights governed by existing areas of law that do not expressly extend to student-athlete biometric data.[8] For example, the

---

7. *Id.* Schools with similar contractual deals involving student-athlete biometric data included: Rutgers, UNLV, Texas at El Paso, Middle Tennessee, Michigan, Louisiana State, Clemson, Minnesota, Tennessee, Utah State, and Boise State. *Id.*

8. Robyn Feldstein et al., *Wearables in the Arena: The Shifting Legal Landscape Governing Fitness Trackers in Professional Sports*, JD SUPRA (Dec. 18, 2018), https://www.jdsupra.com/legalnews/wearables-in-the-arena-the-shifting-89206/. Although the NCAA and its member institutions govern the use of student-athlete data collected through wearables, this governance is limited to performance and does not extend to limitations on commercial use. *Id.* The NCAA allows wearables in games but prohibits using real-time data analysis to the extent that it is used for the purposes of making performance-enhancing adjustments. *Id.*; *see also* THE NAT'L COLLEGIATE ATHLETIC ASS'N, NCAA SWIMMING AND DIVING 2019–20 AND 2020–21 RULES BOOK 32–33 (Greg Lockard et al. eds., 2019), http://www.ncaapublications.com/productdownloads/SW20.pdf ("The use of technology and automated data collection devices 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."); THE NAT'L COLLEGIATE ATHLETIC ASS'N, NCAA WOMEN'S BASKETBALL 2019–20 AND 2020–21 RULES BOOK 98, http://www.ncaapublications.com/productdownloads/WBR20.pdf (using data results in a technical foul and making the exception for "[e]lectronic transmission of data pertaining to the health and safety of a player may be transmitted to the medical staff in the bench area, but may not be shared with the coaching staff for coaching purposes.); THE NAT'L COLLEGIATE ATHLETIC ASS'N, NCAA MEN'S BASKETBALL

use of this same kind of data is expressly protected in the consumer context under some state laws and in the professional athlete context within collective bargaining agreements.[9] These laws serve as a guidepost for identifying the manner in which the law should govern student-athlete biometric data. In mirroring ABD protection in the consumer and professional athlete contexts, current legislation provides a legal framework to draft comprehensive legislation to ban the monetization of the data and prohibit student athletes' waiver of their ABD rights in an age where sports analytics has turned its radar to the profitability of wearables.

This Note proceeds in five sections, with this introduction serving as Part I. Part II defines ABD and explores current laws regulating the use of biometric data. Part III examines the role of player autonomy in directing the collection and use of ABD and further addresses privacy concerns in the absence of student-athlete biometric data regulation. Part IV suggests a ban on the monetization of ABD without meaningful player consent and presents a legal framework for regulating student-athlete biometric data while still realizing a student-athlete's right to profit from their ABD. Part V briefly concludes and illustrates how the proposed ban applies to everyday student-athletes.

II. EXPLORING ABD

ABD is a gateway to understanding performance through the lens of metrics unique to individual student-athletes. A clearer understanding of heightened performance and quicker recovery is achieved through access to biometric data captured through wearables. Laws can and do exist to regulate biometric data for consumer protection. Yet, laws must set out limitations for NCAA institutions

---

2019–20 CASE BOOK 86, http://www.ncaapublications.com/productdownloads/BKBCB20.pdf (permitting "enter[ing] the game wearing a device that the team's medical staff certifies is worn for medical decision-making" but precluding the medical staff from sharing the information with coaching staff during the game for purposes other than player health and safety); THE NAT'L COLLEGIATE ATHLETIC ASS'N, NCAA CROSS COUNTRY/TRACK AND FIELD 2019 AND 2020 RULES 61, http://www.ncaapublications.com/productdownloads/TF20.pdf (prohibiting the us[e of] any device or technology that provides the user with an unfair advantage over another athlete).

9. *See* discussion *infra* Sections III.B.1, III.B.2.

and third parties with access to ABD. With wearables widely used across NCAA member institutions, a ban on the monetization of ABD without meaningful consent from student-athletes properly recognizes the far-reaching potential of the collection, use, and storage of student-athlete biometric data.

A. Access to Biometric Data through Wearables

To understand the breadth of biometric privacy, it is imperative to note the distinction between biometric *data* and biometric *identifiers*—the first data type of electronic personal data to be protected by law.[10] These terms are subsets of biometric information, are not one in the same, and the term used within a given law depends on the information captured.[11] Biometric identifiers refer to retina scans, fingerprints, and handprints.[12] By contrast, biometric data is defined as "the measurement and analysis of unique physical or behavioral characteristics," which may be physiological (such as heart rate or temperature) or behavioral, "especially as a means of verifying personal identity."[13] Biometric data is a category of personal data implicated through the collection of ABD, which captures measurements or records identifying individual performance data unique to student-athletes.[14]

---

10. *See* Barbara Osborne, *Legal and Ethical Implications of Athletes' Biometric Data Collection in Professional Sport*, 28 MARQ. SPORTS L. REV. 37, 38 (2017), https://scholarship.law.marquette.edu/cgi/viewcontent.cgi?article=1719&context=sportslaw.

11. *Id*; *see* discussion *infra* Section B (exploring state regulation of biometric data privacy and illustrating the differentiation of the data captured within the definitions of biometric identifier and biometric data therein).

12. Illinois Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14/10 (2020); *see also* Nicholas Zych, *Collection and Ownership of Minor League Athlete Biometric Data by Major League Baseball Franchises,* 14 DEPAUL J. SPORTS L. 129, 153 (2018) ("The current BIPA definition of 'Biometric Identifier' encompasses 'a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.'" (quoting section 10 of the Act)).

13. *Biometrics*, MERRIAM-WEBSTER, https:www.merriam-webster.com/dictionary/biometrics (last visited Oct. 24, 2019); Osborne, *supra* note 10.

14. *See* Osborne, *supra* note 10, at 37–38.

Collecting ABD is not a new frontier in sports. Teams routinely harness "a wide variety of biometric and biomechanical measurements, including vertical jump, pitch speed, reaction time, heart rate, body composition, and self-reported wellness information."[15] The foundational purposes of ABD remain: (1) to optimize player performance, health, and wellness, and (2) to prevent injuries.[16] More recently, however, use of this data has evolved into a revenue source

15. *Id.*
16. *Id.* at 40.

and offers additional avenues for fan engagement, sponsorship deals,[17] and even a competitive edge in fantasy sports.[18]

---

17. Sam Adams, *Wearable Technology in Sport*, COOPER GRACE WARD (Aug. 12, 2019), https://www.cgw.com.au/publication/wearable-technology-in-sport/. In addition to health and performance benefits, biometric data presents platforms for fan engagement and sponsorship deals in sports:

> For sporting fans, performance statistics are already an important part of the game. For example, batting averages, strike rates, tackles, disposals, distance gained, first downs, and percentage of shots made. Adding biometric markers to these statistics will provide some unique insights that help fans feel closer to their heroes.
>
> Biometric data has the potential to become extremely valuable property that could be commerciali[z]ed by: sporting administrators to improve fan engagement and to seek quantitative analysis around player performance and injury management; media companies as a way of delivering a better fan experience; punters and wagering companies using predictive analysis to detect trends that are important in jurisdictions that allow live in-play betting; [and] sports integrity operators looking to identify potential flags for corrupt activities.
>
> Sports administrators are best placed to manage many of these relationships, particularly with broadcast partners and as a way of enhancing fan engagement. From an injury management and player performance perspective, player associations [and the NCAA] may have concerns about how widely the information is shared.
>
> . . . .
>
> For sports stars, the combination of biometric data and unprecedented consumer demand for wearable technology to deliver health and fitness goals provides athletes with a unique new source of revenue. Critically, this opportunity is something that could provide a lucrative revenue stream both during and after the conclusion of a playing career.
>
> . . . .
>
> Athletes can use biometric data to show their fans (or people wanting to learn how to become high performers) what was happening inside their bodies in moments of immense pressure. At the same time, they can commentate about the mental exercises they undertook in order to regulate their biometric rhythm. Through the massive reach of social media, athletes can speak with authenticity and build an audience that commerciali[z]es their unique knowledge

Today, ABD is commonly captured through wearables and is widely used at all levels of sports, including professional, college, and high school athletics.[19] As illustrated in Asia's story, wearables are smart devices typically sewn into clothing or installed in an accessory such as a mouth guard or pitching sleeve.[20] The wireless device transmits data to an internet source and monitors various sources of information unique to the wearer, such as sleep patterns, heart rate, glucose levels, and other personally identifiable physical and physiological data points for the purposes of assessing recovery and performance in sports.[21] Given the exponential growth of wearables and rapid developments in technology expanding their capabilities, legislation and the NCAA are behind the curve on governing their use in college sports.[22]

> in a way that sustains them after the conclusion of their sporting careers.

Id.

18. The NCAA successfully struck an agreement with online sports gambling powerhouses FanDuel and DraftKings to forgo drafting proposed regulations for a ban on betting in college sports. *See* Dustin Gouker, *Why Are DraftKings and FanDuel Discontinuing College Fantasy Sports Contests?*, LEGAL SPORTS REP. (Mar. 31, 2016), https://www.legalsportsreport.com/9382/draftkings-fanduel-and-ncaa/; *see also* Paul R. La Monica, *DraftKings Looks to Profit from Legal NCAA Tournament Bets*, CNN BUSINESS (Mar. 18, 2019, 3:41 PM), https://www.cnn.com/2019/03/18/investing/ncaa-tournament-legal-gambling-draftkings-new-jersey/index.html. This agreement is unlikely to be upheld because of the Supreme Court's legalization of college sports betting. *See* discussion *infra* Section III.B.2. Nevertheless, the NCAA should likewise follow suit and work with FanDuel and DraftKings to continue discussions on proposing regulations on college sports betting with a goal to protect the future of ABD integration in the fan experience. This legislation should include student-athlete player consent as this Note proposes.

19. Joseph J. Lazzarotti et al., *As Wearable Technology Booms, Sports and Athletic Organizations at All Levels Face Privacy Concerns*, JACKSON LEWIS (Apr. 5, 2019), https://www.workplaceprivacyreport.com/2019/04/articles/health-information-technology/as-wearable-technology-booms-sports-and-athletic-organizations-at-all-levels-face-privacy-concerns/ (discussing laws implicated when organizations collect, use, and store ABD).

20. *See* Feldstein et al., *supra* note 8.

21. *Id.*

22. *Id.*

B. Biometric Data Protection Laws and Regulation

Few states regulate the collection and retention of biometric data in general and no state regulates ABD at the collegiate level.[23] Illinois, Texas, and Washington only protect biometric identifiers, which include data captured from retina scans, fingerprints, and handprints.[24] By contrast, states protecting biometric data guard personal information "comprised of unique biological and behavioral characteristics that identify a specific individual."[25] This means that biometric data is not categorically identified as a biometric identifier and therefore not safeguarded under any law that expressly protects biometric identifiers by definition. Despite ABD falling outside the scope of any laws governing biometric identifiers, understanding the legislative landscape of biometric information is critical to addressing ABD monitoring at the collegiate level and crafting state legislation that broadly governs biometric data.

1. State Action: Utilizing the Legislative Landscape of Biometric Data as a Framework

While the exact metrics used to define biometric data may vary from one legislative framework to the next, the policies for identifying and protecting the data are largely the same. The Illinois Biometric Information Protection Act ("BIPA") policy states: "[t]he public

23. *See* Katrina Karkazis & Jennifer R. Fishman, *Tracking U.S. Professional Athletes: The Ethics of Biometric Technologies*, 17 AM. J. BIOETHICS 45, 45–60 (2017), https://www.researchgate.net/publication/311766578_Tracking_US_Professional_Athletes_The_Ethics_of_Biometric_Technologies (noting that use of biometric technology in professional sports remains "largely unregulated and unexamined"); *see also* Molly K. McGinley et al., *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, NAT'L L. REV. (Mar. 25 2019), https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states; Zachary Zagger, *States on Deck to Protect College Athlete Biometric Privacy*, LAW360 (Oct. 24, 2019), https://www.law360.com/articles/1212731/states-on-deck-to-protect-college-athlete-biometric-privacy.

24. *See* McGinley et al., *supra* note 23.

25. 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. SPORTS & ENT. L. J. 7, 12 (2016).

welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[26] Recognizing the need to expand the definition of a biometric identifier to expressly include the biometric data captured by wearable devices that are currently left unprotected, a proposed bill seeks to broaden the Illinois statutory definition of biometric identifier to include "an electrocardiography result from a wearable device."[27] Thus, the Illinois bill would effectively protect biometric identifiers and biometric data within its statutory scope, at least to the extent the data is collected from a wearable device.

State legislative responses to the growth of biometric data usage also focus on prohibiting the use of consumer biometric data use for marketing purposes. Arizona, California, Florida, and Massachusetts have joined Illinois, Texas, and Washington by either enacting or proposing legislation addressing biometric data privacy.[28] Arizona's bill proposes a prohibition on the commercial use of a biometric data identifier.[29] Under the Massachusetts bill, biometric data encompasses any personal information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or the consumer's

---

26. Illinois Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14/5(g) (2020).

27. *See* Jeffrey D. Neuburger, *Recent Bill Introduced in Illinois Legislature Would Curtail BIPA Litigation*, NAT'L L. REV. (Mar. 28, 2019), https://www.natlawreview.com/article/recent-bill-introduced-illinois-legislature-would-curtail-bipa-litigation. The BIPA only includes the definition of a biometric identifier, which it defines as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILL. COMP. STAT. 14/10 (2020). However, although the statute does not expressly define biometric data, biometric data could be interpreted to fall under the BIPA's definition of biometric information. *See id.* (defining biometric information 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").

28. *See* McGinley et al., *supra* note 23.

29. *Id.*

device."[30] The bill also broadly defines biometric data to include both biometric identifiers and biometric data.[31]

Some states also impose breach notification and consent obligations on entities collecting biometric data. For instance, Colorado, Maryland, North Carolina, and Wisconsin require notification of a breach of biometric data within a reasonable time.[32] Regarding consent, Illinois' BIPA is the only biometric privacy law that mandates notice and consent prior to capture—regardless of whether it is used for a commercial purpose.[33] Washington, Texas, and Arizona require notice and consent only if the data is captured for a commercial purpose.[34]

Legislation that covers important aspects of biometric data not only aids the law's ability to maintain pace with the growth of capturing biometric data but also attempts to anticipate the breadth of protection needed to account for unforeseen technological advances.[35] To do so, legislation must broadly define biometric data.[36] Comprehensive

---

30. *Id.*

31. *Id.* (defining biometric data to include biometric identifiers (such as retina scans, handprints, and fingerprints) but also biometric data (such as keystroke or gait patterns or rhythms, as well as sleep, health, or exercise data containing identifying information)).

32. *See* COLO. REV. STAT. § 6-1-716(2) (2020) ("without unreasonable delay"); MD. CODE ANN., COM. LAW §14-3504(b)(3) (West 2020) ("as soon as reasonably practicable, but not later than 45 days after the business concludes the investigation" mandated under the statute upon discovery or notification of a breach of personal information); N.C. GEN. STAT. § 75-65(a) (2020) ("without unreasonable delay"); WIS. STAT. § 134.98(3)(a) (2020) ("within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information").

33. McGinley et al., *supra* note 23 n.6 ("Of the current biometric privacy laws in place, only Illinois BIPA requires notice and consent for the capture of a biometric identifier, regardless of the purpose, while Washington State, Texas, and [Arizona] require notice and consent only if the identifier is to be used for a commercial purpose.").

34. *Id.*

35. Duane C. Pozza & Kathleen E. Scott, *Biometrics Laws Are on the Books and More Are Coming: What You Need to Know*, WILEY (Apr. 2019), https://www.wileyrein.com/newsroom-newsletters-item-Apr_2019_PIF-Biometrics-Laws-Are-on-the-Books-and-More-Are-Coming-What-You-Need-to-Know.html#_ftn7.

36. *Id.* (noting the CCPA "sweeps in biometric data in its broad definition of 'personal information'").

biometric privacy legislation "create[s] specific notice, consent, security, and other requirements for the collection, use, and sharing of biometric data."[37] Furthermore, to truly safeguard biometric data, the collection and retention of biometric data specifically must be an element that on its own "triggers a notification requirement[] in the event of a data security breach."[38] Summarily, a broad state legislative scope governing student-athlete biometric data anticipates technological advances; recognizes that some states only protect biometric identifiers; and accommodates for that distinction to better protect data captured through biometric data monitoring by adequately defining biometric data to include physiological and behavioral characteristics linked to sports performance.

2. California Consumer Privacy Act ("CCPA")

The CCPA is the most comprehensive legislation dealing with biometric data usage.[39] The CCPA regulates the collection, retention, and distribution of personal information, which is defined in the statute to include biometric information and broadly sweeps a host of personal information relating to both biometric identifiers and biometric data.[40] Under the CCPA "[b]iometric 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,

---

37. *Id.* (citing 740 ILL. COMP. STAT. 14/5 (2020); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2020); WASH. REV. CODE § 19.375 (2020)).

38. *See* Pozza & Scott, *supra* note 35 (citing ARIZ. REV. STAT. § 18-551(11)(i) (2020); COLO. REV. STAT. § 6-1-716(1) (2020); DEL. CODE ANN. tit. 6, § 12B-101(7) (2020); 815 ILL. COMP. STAT. 530/5 (2020); IOWA CODE § 715C.1(11)(a)(5) (2020); LA. STAT. ANN. § 51:3073(4)(a)(v) (2020); NEB. REV. STAT. § 87-802(5)(v) (2020); N.M. STAT. ANN. § 57-12C-2(A), (C) (West 2020); S.D. CODIFIED LAWS § 22-40-19(4)(e) (2020); WIS. STAT. § 134.98(b) (2020); WYO. STAT. ANN. § 6-3-901(b) (2020)).

39. *See* Alan L. Friel & Niloufar Massachi, *California Passes Groundbreaking Data Privacy Law Granting Consumers Expansive Privacy Rights*, BAKER HOSTETLER DATA COUNSEL (July 3, 2018), https://www.dataprivacymonitor.com/advertising/california-passes-groundbreaking-data-privacy-law-granting-consumers-expansive-privacy-rights/.

40. California Consumer Privacy Act (CCPA) of 2018, CAL. CIV. CODE § 1798.140(b) (West 2020) (defining biometric information).

and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information."[41] Biometric information, as used here, incorporates "exercise or health data . . . which means data collected by wearables is likely to be subject to a host of regulations."[42]

Among other statutory thresholds, a business is subject to CCPA regulation if the business collects consumer personal information; does business in the State of California; and has an annual gross in revenue exceeding $25,000,000.[43] Because the CCPA applies to businesses, the statute could apply to a professional sports team or an organization collecting data of an athlete who resides in California, and the organization need not be located in California.[44] In particular, the CCPA prohibits a person from waiving biometric data rights, potentially affecting a team's ability to monetize player data.[45] Because ABD monitors the type of data current laws protect, the CCPA suggests third parties contracting to collect student-athlete biometric data, with NCAA institutions as conduits facilitating access to the data, are likely prohibited from monetizing the ABD. This means current contractual agreements between NCAA programs and third parties like Nike may very well run afoul of biometric data privacy protection under the CCPA[46] and many other biometric data privacy laws upon further examination.[47] To fill the legislative gap governing student-

41. *Id.*

42. *See* Feldstein et al., *supra* note 8.

43. CCPA, CIV. CODE § 1798.140 (c)(1)(A) (defining "business" within the meaning of the CCPA and entity actions surrounding the collection of consumer personal information that triggers CCPA regulation).

44. *See* Lazzarotti et al., *supra* note 19.

45. *Id.*

46. CCPA, CIV. CODE § 1798.192 (prohibiting waiver of biometric data rights and rendering a contract or provision purporting to do so void as against public policy). According to Forbes, the University of Southern California's football program generated a three-year average of $93 million in revenue between the 2015–2016 and 2017–2018 seasons. Chris Smith, *College Football's Most Valuable Teams: Reigning Champion Clemson Tigers Claw into Top 25*, FORBES (Sept. 12, 2019, 6:00 AM), https://www.forbes.com/sites/chrissmith/2019/09/12/college-football-most-valuable-clemson-texas-am/#4f386b89a2e7.

47. Given the recent development of state statutes governing biometric data, the author suggests that much like the prohibited waiver of rights under the CCPA, a

athlete biometric data, Major League Baseball's regulation of ABD is illustrative of a solution to the NCAA's regulatory void of NCAA institutions commercializing student-athlete biometric data.

3. Major League Baseball

Tracking the existing Illinois BIPA, Major League Baseball's ("MLB") collective bargaining agreement ("CBA") properly recognizes the need to ban the monetization of ABD. In broadening its definition of biometric data to include performance metrics, MLB currently bans any commercial use of ABD by a "Club," Major League Baseball, or any Major League Baseball-related entity or other third party as this Note proposes.[48] MLB's preemptive step to ban the monetization of ABD illustrates a working framework and realization that such data should be protected from the economic gain of third-parties and used primarily for health and performance benefits unless such use is authorized with meaningful consent, as this Note advocates.[49] ABD should be used at the sole discretion of the student-athlete who will be empowered to either accept the opportunity to profit off their ABD or prohibit any other entity from monetizing ABD captured through various channels, such as wearables, and instead limit the tracking to health and performance purposes, or prohibit the monitoring completely.

---

closer survey of biometric data privacy laws of other states will likely reveal other areas where the monetization of student-athlete biometric data is improper.

48. The MLB CBA provides that "[a]ny commercial use or exploitation of such [ABD] by a Club, Major League Baseball, or any Major League Baseball-related entity or other third party is strictly prohibited." *See* Zych, *supra* note 12, at 136 (quoting Letter from Matthew R. Nussbaum, Assistant General Counsel, Major League Baseball Players Ass'n, to Chris Marinak, Senior Vice President, Econ. & Strategy, Off. of the Commissioner of Major League Baseball, Attachment 56 to the 2017–2021 BASIC AGREEMENT 335 (Dec. 1, 2016) [hereinafter BASIC AGREEMENT], https://www.dol.gov/sites/dolgov/files/olms/regs/compliance/cba/2019/private_/30majorclubs_k9831_060122.pdf.

49. The MLB CBA requires a "written explanation of the technology being proposed, along with a list of the Club representatives who will have access to the information and data collected, generated, stored, and/or analyzed." *See* Zych, *supra* note 12, at 136 (quoting BASIC AGREEMENT, *supra* note 48, at 334). The MLB CBA also directs the destruction of ABD upon a player's request and also gives the player the option to request a copy of the data. *See id.* at 148.

C. General Wearables Usage among NCAA Institutions

Many NCAA institutions have adopted the use of wearables.[50] Uses range "from mouth guards with built-in sensors measuring hits in football to the Catapult devices used in the professional leagues."[51] WHOOP, Catapult, and Firstbeat are among the most common corporations supplying wearables to NCAA institutions to collect student-athlete biometric data.[52] Unique market positioning enables these companies to leverage the use of their products to access the data the wearables collect—making student-athletes walking laboratories for profit.

1. WHOOP

Fifty teams at twelve institutions have adopted the WHOOP program.[53] The WHOOP wristband is "the most ambitious continuous-monitoring device on the market,"[54] as it continuously measures recovery, strain, and sleep.[55] The wristband allows student-athletes to track behavioral changes such as sleep, recovery, alcohol intake, caffeine consumption, and sexual activity daily—crossing the line to

50. Understanding that corporations stand to profit from the monetization of ABD further demonstrates the far-reaching effects of ABD commodification.

51. Cameron Miller, *Surveying Biometric Data Privacy, Ownership, and Usage in American Sports*, U. OF DENV. SPORTS & ENT. L. J. (Apr. 11, 2018), https://duselj.wordpress.com/2018/04/11/surveying-biometric-data-privacy-ownership-and-usage-in-american-sports/.

52. Shourjya Sanyal, *How Are Wearables Changing Athlete Performance Monitoring?*, FORBES (Nov. 30, 2018, 08:56 PM), https://www.forbes.com/sites/shourjyasanyal/2018/11/30/how-are-wearables-changing-athlete-performance-monitoring/#d2922d8ae095 (discussing wearable tracking device companies used to collect ABD); *see also* 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, 90 (2019) (noting that while Nike announced a departure from the wearables industry, it is still able to track biometric data through the Nike+ app).

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

54. *Id.*

55. *Experience*, WHOOP, https://www.whoop.com (last visited Oct. 24, 2020).

invasive.[56] Thereafter, "[t]he metrics are published to a dashboard accessible by users and coaches to calculate an athlete's 'recovery level,' providing insight into how to manage an athlete's optimal daily performance level."[57]

While WHOOP wristband's constant monitoring of student-athlete biometric data raises personal privacy concerns,[58] athletic programs such as The University of Tennessee have experienced the positive outcomes WHOOP touts.[59] Tennessee swimming and diving coach Matt Kredich credited student-athlete Kira Toussaint's performance improvements resulting from monitoring her recovery metrics to WHOOP use.[60] Toussaint "had some of the lowest recovery scores on the team, but she was persistent about checking the data and adjusting her sleep and workouts based on the results."[61] Within one season, she surpassed school records and clocked a qualifying time for the Rio Olympics, demonstrating the value wearables provide in relation to performance improvement.[62] Other devices allow the same ability to monitor performance data while focusing solely on competition and practice activity, avoiding WHOOP's invasive and continuous monitoring.

2. Catapult

The Australian company, Catapult, is another wearable device company used among most NCAA institutions. Programs are better able improve student-athlete health and performance by assessing metrics acquired through a GPS sensor worn on an athlete's back.[63] In 2018, more than 1,500 teams across 35 sports used Catapult wearable

---

56. Shultz, *supra* note 53. WHOOP tracking raises more privacy concerns and puts extremely personal details on display such as "teammates being privy to intimate details of one another's sex lives and other late-night endeavors." *Id.*

57. Jessop & Baker, *supra* note 52, at 88.

58. *See supra* note 56 and accompany text.

59. Shultz, *supra* note 53.

60. *Id.*

61. *Id.*

62. Jessop & Baker, *supra* note 52, at 88–89.

63. *Id.* at 87.

hardware.[64] Among 372 universities, 584 teams are Catapult clients,[65] including Duke Basketball, all 19 programs at Baylor University, and nearly half of the top 5 NCAA Division I football teams.[66]

Catapult's wearable technology allows programs to maximize performance, minimize injury risk, and "objectively manage the rehabilitation process."[67] To mitigate the impact of injuries, Florida State University invested $80,000 in thirty Catapult GPS sensors for use during practice and games, becoming Catapult's first NCAA football client in 2012.[68] Sizeable investments in wearables enable NCAA institutions to ensure student-athletes are healthy for competition, and teams attribute the student-athlete's success to the device's capabilities.[69]

3. Firstbeat

Firstbeat monitors heart rates. The company's "textile heart-rate belt, plastic heart-rate belt, and team receiver use a chest strap based system to track [a] user's heart rate and heart rate variability."[70] Using Firstbeat enables a team to assess "primary biometric parameters to derive detailed information about the athlete's training loads, performance readiness, fitness testing, sleep quality, and lifestyle."[71] Over 22,000 athletes among 1,000 teams around the world rely on

---

64. *Id.*

65. *Catapult Reaches Major Milestone Passing 1,000 Teams in North America*, CATAPULT (Aug. 16, 2019), https://www.catapultsports.com/blog/catapult-reaches-major-milestone-passing-1000-teams-in-north-america.

66. Jessop & Baker, *supra* note 52, at 87.

67. *Wearable Technology*, CATAPULT, https://www.catapultsports.com/products (last visited Oct. 24, 2020); *User Stories*, CATAPULT, https://www.catapultsports.com/customer-stories/baylor-university (explaining Baylor University's adoption of the full performance platform which includes wearable technology, athlete management, and video analysis) (last visited Oct. 24, 2020).

68. Jessop & Baker, *supra* note 52, at 87. Former Florida State University head football coach Jimbo Fisher credits the team's undefeated 2014 championship season to Catapult's GPS sensors, stating, "I think [ABD tracking] has been very critical to our development since it keeps guys on the field." *Id.* at 88.

69. *Id.* at 87.

70. Sanyal, *supra* note 52.

71. *Id.*

Firstbeat for peak performance.[72] This includes ninety-nine NCAA soccer, ice hockey, basketball, lacrosse, tennis, rowing, field hockey, volleyball, baseball, wrestling, track & field, and softball programs.[73]

Wearable metrics are beneficial to both coaches and athletes in that they provide meaningful insight about athletic performance, stress, rest, and recovery.[74] However, the terms of use agreements "for ABD collection devices were drafted for consumers rather than NCAA athletes" and, therefore, "do not adequately notify NCAA athletes of the contractual risks shifted to them in their use of ABD collection devices."[75] Student-athletes must have meaningful consent when granting access to their personal data and a voice in how ABD is used along with the autonomy to position ABD as a tool for sponsorship endorsements as wearable industry trends project exponential growth and the amateurism model changes to allow for NIL profits.

---

72. *Id.*

73. *See Firstbeat Sports – Client List*, FIRSTBEAT, https://www.firstbeat.com/en/client-list/ (listing numerous NCAA institutions as clients) (last visited Oct. 24, 2020).

74. *See* Sanyal, *supra* note 52.

75. Jessop & Baker, *supra* note 52, at 108. Further describing their findings resulting from examining student-athlete biometric data collection contracts, Jessop and Baker explain:

> The Terms of Use agreements built into applications for ABD collection devices were drafted for *consumers rather than NCAA athletes*. Therefore, such agreements do not adequately notify NCAA athletes of the contractual risks shifted to them in their use of ABD collection devices. Courts have failed to find adequate notification of substantial risks incorporated in the shrink-wrapped terms found in standardized agreements. The warnings and disclaimers found in the Terms of Use agreements for ABD collection devices are not specific to or inclusive of the risks related to NCAA athlete use of ABD collection devices discussed in this article. Furthermore, [their] review of the opt-in process revealed that participating institutions direct NCAA athletes to download the applications but do not provide any additional clarification or notification of the standardized terms of use.

Id. (emphasis added).

III. WHERE PROFITS & PRIVACY INTERSECT: WEARABLES AS A REVENUE SOURCE FOR PLAYERS AND A PLATFORM FOR PLAYER AUTONOMY

Commercialization of student-athlete biometric data is currently a one-way street with NCAA programs and third parties realizing its profits. Instead, whether an entity enjoys profits from such personal and invasive information should be subject to the sole discretion of student-athletes. A ban on the monetization of student-athlete biometric data without meaningful player consent better protects student-athlete privacy interests while still harnessing the goal of improving health and maximizing performance. The Ninth Circuit's decision in *O'Bannon v. NCAA* and subsequent NCAA developments permitting student-athletes to profit from their NILs suggest that ABD presents a revenue source for student-athletes.[76] Should a student-athlete opt to share ABD metrics, doing so could present the opportunity to profit in an industry where competition to track ABD continues to rise.[77]

A. Athlete Biometric Data and Intellectual Property Law

Autonomy over wearables data usage provides student-athletes an avenue to profit from their ABD akin to their NILs in the wake of *O'Bannon v. NCAA*.[78] In *O'Bannon*, current and former NCAA players alleged the NCAA's fixed pricing of student-athletes' NILs constituted an illegal restraint on competition in the marketplace and thereby

76. *See* O'Bannon v. NCAA, 802 F.3d 1049 (9th Cir. 2015); *infra* notes 84–88 and accompanying text.

77. *See* Jessop & Baker, *supra* note 52, at 89–90 (explaining the competition between two major sport apparel companies, Nike and Under Armour, to control the ABD-collection market).

78. *See* 802 F.3d at 1053 (agreeing with the lower court that the NCAA's compensation rules are subject to antitrust scrutiny); *see also* David Hale & Myron Medcalf, *NCAA Explores Compensation for Names, Likeness*, ESPN (May 14, 2019), https://www.espn.com/college-sports/story/_/id/26747489/ncaa-explores-compensation-names-likeness; David K. Li, *NCAA Takes Steps To Allow College Athletes To Cash in on Their Fame*, NBC NEWS (Oct. 29, 2019, 1:21 PM), https://www.nbcnews.com/news/us-news/ncaa-takes-steps-allow-student-athletes-cash-their-fame-n1073436.

violated the Sherman Antitrust Act.[79] The Ninth Circuit agreed with the student-athletes and largely with the district court's remedies.[80] The court concluded "the district court correctly identified one proper alternative to the current NCAA compensation rules—*i.e.*, allowing NCAA members to give scholarships up to the full cost of attendance—but that the district court's other remedy, allowing students to be paid cash compensation of up to $5,000 per year, was erroneous."[81] *O'Bannon* explained that the district court "clearly erred when it found that allowing students to be paid compensation for their NIL[] [licenses] is virtually as effective as the NCAA's current amateur-status rule."[82] Although *O'Bannon* refused to allow student-athletes to receive compensation for their NILs, the decision took "the first step towards this new paradigm in college athletics."[83]

In response to *O'Bannon*, state action,[84] and the current amateurism debate in college sports, the NCAA Board of Governors voted unanimously to allow student-athletes to receive compensation for their NILs "in a manner consistent with the collegiate model."[85]

---

79. *See* O'Bannon v. NCAA, 7 F. Supp. 3d 955, 962–63 (N.D. Cal. 2014) (providing an introduction to plaintiffs' claims against the NCAA), *aff'd in part, rev'd in part by* O'Bannon, 802 F.3d at 1053.

80. *See O'Bannon*, 802 F.3d at 1053.

81. *Id.*

82. *Id.* at 1074.

83. *See* Michael Steele, Comment, O'Bannon v. NCAA*: The Beginning of the End of the Amateurism Justification for the NCAA in Antitrust Litigation*, 99 MARQ. L. REV. 511, 524 (2015); *see also* 2020–2021 NCAA DIVISION I MANUAL 62–63, 71, https://web3.ncaa.org/lsdbi/reports/getReport/90008 (stating that to maintain amateurism status, "an individual shall not . . . enter[] into any kind of agreement to compete in professional athletics, either orally or in writing, regardless of the legal enforceability of that agreement," and must abide by the rules and policies when compensation is allowed).

84. *See infra* note 165 (discussing state bills allowing student-athlete compensation for the use of their NILs).

85. Press Release, NCAA, Board of Governors Starts Process to Enhance Name, Image, and Likeness Opportunities (Oct. 29, 2019), http://www.ncaa.org/about/resources/media-center/news/board-governors-starts-process-enhance-name-image-and-likeness-opportunities. The NCAA Board of Governors' vote allows all college athletes the opportunity to profit from the use of their NILs and does not affect student-athlete amateurism status. The student-athlete's right to profit off of the use of their NIL is not immediate. *Id.* To effectuate the decision, the Board delegated the promulgation of the rules regulating NIL profits to

The Board based this action on input gathered by the NCAA Board of Governors Federal and State Legislation Working Group from current and former student-athletes, university presidents, faculty, coaches, and commissioners representing all three NCAA divisions.[86] To implement the approval for student-athlete NIL compensation, the NCAA also directed the working group to maintain continued engagement with legislators to gather insight on how to further refine the principles and regulatory framework governing NIL.[87] The goal of this charge is to ensure principles and policies are responsive to state and federal legislation.[88]

---

the NCAA's three divisions. *Id.* Thus, the right to profit from NILs is still pending as no NCAA division has yet to finalize its rules regulating the parameters of student-athlete compensation. *Id.*

86. *See* Press Release, NCAA, *supra* note 85.

87. *Id.* University presidents, commissioners, athletics directors, administrators, and student-athletes also make up the working group established to maintain ongoing engagement with state legislators. *Id.*

88. *See id.*; Ross Dellenger, *Congress, the NCAA, and Athlete Compensation Is a Battle Far from Over*, SPORTS ILLUSTRATED (Apr. 27, 2020), https://www.si.com/college/2020/04/27/ncaa-name-image-likeness-debate-congress. There is a race among Congress and states to pass legislation governing NILs, yet still no proposal mentions ABD. *Id.* The NCAA urges Congress to act quickly and intervene to prevent the state patchwork legislation that is unfolding. *Id.* Some argue NIL governance is a state issue. Those who favor congressional action "disagree on a framework for federal legislation, the timing of such a law, and its ability to pass the slow-moving body." *Id.* Similar to the Court's ruling that legalized gambling was a state issue in *Murphy*, perhaps the Court would hold that regulating NIL use is within the province of the states should the Court take up the issue. *See infra* note 106 and accompanying text (discussing the Court's ruling that legalized gambling is a state issue); Joseph W. Swanson et al., *Be Prepared for the Next Wave of Biometric Data Laws: Five Tips for Businesses*, CARLTON FIELDS (Mar. 20, 2019), https://www.carltonfields.com/insights/publications/2019/be-prepared-next-wave-biometric-data-laws#:~:text=Congress%20and%20state%20legislatures%20are%20considering%20new%20laws,and%20the%20Fair%20Credit%20Reporting%20Act%2C%20among%20others. While "Congress and state legislatures are considering new laws to regulate the collection and use of personal data, including biometric data[, c]urrently, there is no federal law that regulates the collection and use of biometric data." *Id.* However, the author still advocates for a state solution for governing student-athlete biometric data because of the current legislative foundation among state law. Nevertheless, should Congress pass a federal law governing biometric data, the model statute proposed in this Note still serves as a framework, as its tenets address the key

Allowing for NIL compensation further evidences the need for a legal grip on collegiate wearable tracking.[89] Intellectual property statutes encompass biometric data and are designed to protect identifying characteristics gathered through ABD.[90] Under intellectual property law, because ABD is personal to an athlete's identity, it should be viewed as an element of a person's NIL; therefore, its sale implicates

---

elements of biometric data collection, use, and storage such that it is suited for adoption at either the state or federal level.

89. *See* O'Bannon v. NCAA, 802 F.3d 1049 (9th Cir. 2015); *see also* Hale & Medcalf, *supra* note 78. Many are saying amateurism is on the way out. The paradigm shift is moving inexorably against the traditional amateurism model. Whether the effect is viewed as an adaptation or extinction, change is coming. Among the dialogue surrounding the NCAA amateurism debate are concerns about the use of student-athlete biometric data. *See, e.g.*, 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/#5ce10f5621cc. Karen Weaver, national-championship-winning former head coach in NCAA Divisions I and III, shares this sentiment:

> Now that California and a host of other states have proposed legislation to undo this, there is one other discussion point that athletes at all levels should seek to own and control—their biometric data. . . .
>
> . . . .
>
> As senior leaders in higher education, our students' personal data is not ours, especially their "biometric" data about physical performance, and should not be for sale as part of an apparel deal, a weight room software package, or any futuristic performance enhancing clothing. Athletic directors especially need to consider the implications of trading off players' personal data for more lucrative contracts (as appears to be the case at Michigan). In effect, data and apparel companies are using college athletes as free research subjects in a for profit enterprise. How is that any different than using their names, images and likenesses?

Id. (emphasis added). While this Note focuses on student-athlete data usage, it fits into the broader conversation surrounding the current state of NCAA amateurism. The author focuses on the student-athlete as opposed to those who profit from the student-athlete, which is appropriate considering that the NCAA amateurism model is changing in favor of the student-athlete.

90. Kristy Gale, *Sports Betting and Biometrics Will Push the Publicity Rights Envelope*, SPORTTECHIE (July 5, 2018), https://www.sporttechie.com/sports-betting-and-biometrics-will-push-the-publicity-rights-envelope-law-legal/.

a right to profit from the use of the ABD.[91] This reasoning skews in favor of student-athletes in the debate over whether amateurism should remain an aspect of college sports as the NCAA's three divisions explore ways to modify its rules and regulations to allow student-athletes to receive compensation for use of their NIL in the wake of *O'Bannon*.[92] As this Note demonstrates, a gap in regulating student-athlete biometric data under existing laws could also lead to a gap in the regulation of student-athlete biometric data as an aspect of NIL compensation unless these rules expressly provide for safeguarding the data.[93] ABD is susceptible to compromised athlete privacy because personal player information is directly linked to ABD.[94] This

---

91. *See* Miranda Stark, Case Comment, *Biometric Data and the Gionfriddo Standard* 5 ARIZ. ST. SPORTS & ENT. L.J. 381, 384–85 (2016) (noting courts would likely treat ABD differently than statistical information due to the invasive nature of the data); *see also* Osborne, *supra* note 10, at 68 (pointing to the NFLPA-Whoop deal, which "ostensibly provides some degree of intellectual property ownership over their ABD and the power to commercialize such data"); Gale, *supra* note 25; Zagger, *supra* note 23; Weaver, *supra* note 89 (arguing that student-athletes own their ABD).

92. See *supra* note 89 and accompanying text for a discussion on recent NCAA developments signaling a move away from the traditional amateurism model and raising ABD as another discussion point.

93. Regulating student-athlete biometric data is on the NCAA's radar. The NCAA approved an Interassociation Task Force on Wearable Technologies that "will work to provide an interassociation pathway to better understand how [ABD] can advance the health and safety of college student-athletes." Report of the NCAA Board of Governors 7 (Aug. 8, 2017), https://www.ncaa.org/sites/default/files/AUG2017BOG_FINALREPORT_20170824.pdf. The Softball Rules Committee, "in consultation with the NCAA Sport Science Institute (SSI) staff, agreed [wearable technology] device[s are] not medically necessary and [are] marketed as a training tool, therefore, rendering it illegal to be worn on the field under Rule 5.9.8." Report of the NCAA Softball Rules Committee Annual Meeting 2 (June 18–20, 2018), https://www.ncaa.org/sites/default/files/Jun2018WSB_Rules_Committee_Annual_Meeting_Report_20180830.pdf.

94. For example, legalized sports betting exposes ABD to a host of privacy risks. Sports programs have demonstrated the value of the data for performance purposes, yet hackers may attack systems to place bets leading to theft of the proprietary information, one of the many unintended consequences of collecting, using, and disseminating ABD. *See generally* William H. Williams, Note, *On the Clock, Best Bet To Draft Cyberdefensive Linemen: Federal Regulation of Sports Betting from a Cybersecurity Perspective*, 13 BROOK. J. CORP. FIN. & COM. L. 539 (2019) (arguing for federal oversight of sports betting).

information is far more sensitive than the use of a student-athlete's NIL.[95] As such, a ban on ABD monetization provides an adequate legal solution grounded in public policy. Further, regulation that guards student-athletes' interests when it comes to ABD protects privacy and ethical interests as well as student-athletes' ability to profit from their ABD because the data has value beyond monitoring performance or gauging recovery levels.

B. Beyond Performance: Commercial Uses for Student-Athlete Biometric Data

Beyond health and performance benefits, access to ABD has other uses. Cultivating fan interest, utilizing metrics for media coverage, and leveraging data within fantasy gaming are among the many ways entities could commercialize ABD.[96] Additionally, "ABD beneficiaries" have an interest in harnessing the potential of ABD.[97] An entity's purpose for using ABD will differ "depending on the role they play in relation to the collection, use, and dissemination of ABD."[98]

1. Fan Engagement

Student-athletes can directly engage with fans through the dissemination of their ABD as a means of connection and motivation.[99]

---

95. *See infra* Section III.C.

96. *See supra* note 13 and accompanying text.

97. *See* Gale, *supra* note 25, at 10. Gale classifies parties with a stake in ABD monitoring as "ABD Beneficiaries" and discusses why ABD is of importance to each stakeholder. "First-Generation Beneficiaries" are "[d]ata controllers including leagues, teams, players associations, and others who collect and control proprietary ABD." *Id.* "Second-Generation Beneficiaries" include data processors like "strategic or investment partners who provide services and capabilities to maximize" ABD use and "vendors who process ABD on behalf of data controllers by obtaining, holding, retrieving, analyzing, utilizing, or disclosing ABD to other third-parties." *Id.* Those entities that are contractually affiliated with data controllers and vendors to use ABD, such as "media, sponsors, endorsers, other licensed content creators," are "Third-Generation Beneficiaries." *Id.*

98. *Id.*

99. *See* Scott Nover & David Cohen, *Sports Leagues Were Already All in on TikTok. Then the Coronavirus Hit*, ADWEEK (Mar. 24, 2020),

For top student-athletes, "the combination of biometric data and unprecedented consumer demand for wearable technology to deliver health and fitness goals provides athletes with a unique new source of revenue."[100] Sharing ABD can demonstrate to fans how an athlete performs under high-pressure situations or recovers from injuries.[101] Student-athletes like Asia can also use the data to show how ABD monitoring helps regulate mental performance.[102]

Student-athletes may also use ABD to connect with fans through social media platforms, allowing them to "speak with authenticity and build an audience" sharing how student-athletes train, what the biometric data shows, and how ABD is used to develop a mindset to perform under high pressure instances.[103] In addition to student-athletes' personal use of ABD for brand-building purposes, media outlets could use ABD to "provide enhanced statistics for live game broadcasts, mobile applications, second-screen platforms, and in-game entertainment for fan engagement."[104] However, a larger platform for fan engagement and one that likely presents the most

---

https://www.adweek.com/digital/sports-leagues-were-already-all-in-on-tiktok-then-the-coronavirus-hit/; *Sports Leagues Using TikTok To Help Connect Players, Fans Amid Virus*, SPORTS BUS. J. DAILY (Mar. 27, 2020), https://www.sportsbusinessdaily.com/Daily/Issues/2020/03/27/Media/TikTok.aspx. Before 2020, it would have been inconceivable for there to be no opportunity for sports fans to interact in person with their favorite sports teams. However, COVID-19 forced sports teams and athletes to turn to social media platforms to stay connected with their fans and realize "their social appeals [were] more important than ever." Nover & Cohen, *supra.* Even "in the weeks before the outbreak shut down much of the United States, executives at most of the major sports leagues emphasized the importance of getting away from highlights on social media and focusing on human-interest stories." *Id.* Sports leagues came to a halt and this halt could have resulted in complete fan withdrawal, but leagues realized this void and responded with encouragement. *Id.* Players posted at-home workouts— such as the National Hockey League's Colorado Avalanche forward Mikko Rantanen lifting his dog—and other mechanisms appealing to the uncertainty the pandemic presented. *Id.* The value of social media influence combined with student-athletes tracking their personal ABD and sharing the data with fans, demonstrates the human-interest aspect student-athlete biometric data provides.

100. *See* Adams, *supra* note 17.

101. *See id.*

102. *See id.*

103. *Id.*; *see also* Gale, *supra* note 25, at 35–37.

104. Gale, *supra* note 25, at 36.

dangerous privacy threat to security lies within fantasy sports and gambling.[105]

2. Sports Betting

Wearables regulation in sports gained more attention following the Supreme Court's decision in *Murphy v. NCAA*.[106] This decision overturned the federal Professional and Amateur Sports Protection Act ("PASPA") of 1992 , clearing the way for legalized sports gambling.[107] *Murphy* deemed PASPA unconstitutional under the Tenth Amendment.[108] Writing for the majority, Justice Alito opined the Court's role is to interpret rather than enact law.[109] PASPA "'regulate[s] state governments' regulation' [of interstate commerce]. . . . The Constitution gives Congress no such power."[110] Following this constitutional charge, PASPA was relegated to a state policy decision.[111] Once free to do so, "several states swiftly acted to legalize sports betting."[112]

ABD technological advances may enhance the fantasy gaming experience "[a]s sports betting becomes more sophisticated and granular, and statistical analytics improve, wearable technology's role will continue to evolve, producing an ever-increasing volume of data

---

105. *See id.* Other potential uses for ABD can be incorporated into "virtual and augmented reality, and other content created by and for the benefit of the Beneficiaries as the sports ecosystem evolves." *Id.* at 36–37. The data "will likely be included in on-screen statistics—providing eSports teams and fans information about opponents that are otherwise unavailable when watching competitors play" as eSports continues to grow. *Id.* at 37.

106. *See* 138 S. Ct. 1461 (2018); Feldstein et al., *supra* note 8 ("Following the Supreme Court's decision in *Murphy v. NCAA*, which overturned the Professional and Amateur Sports Regulation Act and cleared the way for more widespread legalized gambling, the regulation of how wearables may be used has gained attention. Analysis of these developments is complicated by the evolving legal landscape surrounding wearable tech, the privacy implications, and the various types of biometric data it may collect.").

107. *See* Feldstein et al., *supra* note 8.

108. *See Murphy*, 138 S. Ct. at 1485.

109. *See id.*

110. *Id.* (quoting New York v. United States, 505 U.S. 144, 166 (1992)).

111. *See id.* at 1484–85.

112. Williams, *supra* note 94, at 540.

that could affect a betting spread or alter the outcome of a game."[113] It is debatable whether ABD will appeal or even be available to fantasy gamers.[114] On the one hand, some doubt "any league will strike a data deal with its players' association or any gambling providers that would allow books to offer legal sports betting on [ABD] with regards to things like heart rate or velocity of impact on the football field anytime soon."[115] On the other hand, others believe it is possible that gamers could be given access to ABD tracking to place proposition bets[116] as a competitive edge in sports wagering.[117] Ultimately, commercializing ABD in this context raises public policy and moral questions for state regulators to answer soon.[118]

3. Sponsorship Deals

The absence of a union leaves student-athletes without a voice at the bargaining table when sponsorship deals between NCAA institutions and companies involve ABD.[119] Contracts signed among NCAA programs and apparel brands offer little insight into how biometric data is used pursuant to these deals.[120] For example, the Michigan and Nike deal "gives Nike the right to 'utilize' 'Activity Based Information,' which includes speed, vertical leap height, shot attempts, and heart rate, though any utilization of the data must be

113. *See* Melinda L. McLellan et al., *Wearables in Sports: Who Are You Betting on?*, 35 ENT. & SPORTS L. 3, 3 (2019).

114. *Compare* John Holden, *The Major Issues Behind Biometric Data and Its Potential in Legal Sports Betting*, LEGAL SPORTS REP. (June 5, 2019), https://www.legalsportsreport.com/32915/biometric-data-legal-sports-betting/ (doubting leagues will give up ABD's monetary advantages) *with* Adams, *supra* note 17 (presenting the idea that ABD will soon appeal to gamers).

115. Holden, *supra* note 114.

116. A proposition bet "is a wager on an individual player or specific event" and is "now one of the fastest-growing segments of the sports betting industry in the United States." *What is a Prop Bet?—Prop Betting Odds, Tips and Advice*, THE LINES, https://www.thelines.com/betting/prop-bets/ (last visited Oct. 24, 2020).

117. *See* Holden, *supra* note 114.

118. *See id.*; *see also* Zagger, *supra* note 23.

119. *See* Miller, *supra* note 51.

120. *See id.*

approved by Michigan and be 'anonymous and de-identified.'"[121] The UCLA-Under Armour deal gives Under Armour the right to outfit student-athletes with heart rate monitors, digital interactive health or fitness tools, health or fitness wearables, and "athletic apparel, footwear, and accessories with the capability of measuring biometric data" but is silent on the limitations of collection, distribution, or the use of ABD.[122] Additionally, "[s]even Under Armour deals—Cincinnati, Kent State, Maryland, South Florida, Texas Tech, UCLA and Wisconsin—require universities to use its 'biometric' products, or activity monitors."[123] Yet, those deals are silent on provisions governing who has access to the data and the limitations on its use.[124] Similarly, a "handful of Adidas deals have clauses about 'watches' universities are required to use," but the deals do not specify that the watches are provided for ABD tracking.[125]

A few NCAA institutions attempt to demonstrate accountability to safeguard player data by expressly limiting student-athlete biometric data contractually. To illustrate, Michigan's Nike deal gives the university control over what information is shared and further "mandates the data be made anonymous, a clause not found elsewhere."[126] The University of Nevada, Las Vegas contract is the only deal requiring written consent.[127] The Nike-Clemson deal states that "activity-based information must comply with student- and

---

121. *Id.* (citing NIKE ALL-SPORT AGREEMENT 1, 5 (Aug. 1, 2016), https://www.toledoblade.com/attachment/2016/04/26/University-of-Michigan-Nike-contract-2016.pdf). This access is dangerously unfettered, broadly unrestrained, and exhibits little safeguards to protect student-athlete data. Essentially, student-athlete privacy interests outweigh Nike's economic interest, and a legislative safeguard against this practice would prevent similar deals. *See id.*

122. *See* ATHLETIC PRODUCT AND SPONSORSHIP AGREEMENT BETWEEN THE REGENTS OF THE UNIVERSITY OF CALIFORNIA, BY AND ON BEHALF OF THE DEPARTMENT OF INTERCOLLEGIATE ATHLETICS ON ITS LOS ANGELES CAMPUS AND UNDER ARMOUR, INC. 2 (May 20, 2016), https://ca-times.brightspotcdn.com/4f/35/75a8045a4515b387eac7fa8bad17/ucla-ua-agreement-fully-executed.pdf (listing provided company products with the capability of capturing biometric data related metrics); *see also* Tracy, *supra* note 4; Miller, *supra* note 51.

123. Kish, *supra* note 5.

124. *Id.*

125. *Id.*

126. *Id.*

127. *Id.*

medical-privacy laws FERPA and HIPAA."[128] Even though contractual deals and clauses governing the use of student-athlete biometric data include vague language limiting ABD collection and use, as a whole, even vague contractual language is not the norm. Moreover, regulation barring the monetization without student-athlete consent is also needed to guide courts. The various uses of student-athlete biometric data are profitable, yet equally raise privacy concerns such that a ban on the monetization of ABD of student-athletes without meaningful consent would bar profiting and work to prevent security breaches.

C. Recognizing the Legal Implications, Risks, and Unintended Consequences of Student-Athlete Biometric Data Collection and Use

Because ABD is most valuable when used to uniquely identify an individual, any use of student-athlete biometric data likely requires identifying the student-athlete in order to fully realize the value in ABD.[129] But would student-athletes want their personal information shared, even if it would help other student-athletes and the data sharing presents a chance for profit? Many risks and concerns are associated with the use of student-athlete biometric data, and the ever-evolving wearables industry has yet to fully realize the breadth of technological advances as collecting and monitoring capabilities rapidly expand. These include, but are not limited to, privacy breaches, effects on student-athlete earning potential, and meaningful consent to both the NCAA institution and the data monitoring company. Thus, an understanding and realization of the privacy risks as well as ethical

128. *Id; see also* Gilbert Smolenski, Comment, *When the Collection of Biometric and Performance Data on College Athletes Goes Too Far*, 54 WAKE FOREST L. REV. 279 (2019); Williams, *supra* note 94, at 547 ("Under the federal statutory framework of the Health Insurance Portability and Accountability Act (HIPAA), some forms of biometric data are protected only 'when collected by health care providers.' Consequently, teams are responsible for self-regulating astronomically large amounts of personal data."). Notably, ABD includes health information. *See supra* note 15 and accompanying text. While many publications and scholars argue that ABD should be protected under HIPAA, that issue falls outside the scope of this Note. However, the larger issue lies within the public policy addressed by this Note, and such a personal and invasive practice is an improper revenue source for college sports programs.

129. *See* Gale, supra note 25, at 35–37.

implications of leveraging ABD beyond health and performance reasons must accompany the use of ABD.[130]

In addition to risks associated with ABD collection and use, scholars also caution programs to curb their reliance on ABD as questions remain regarding the validity and accuracy of the information captured.[131] Consequently, findings resulting from the data captured through wearables remain unverified.[132] Moreover, "there is currently no standard for evaluating the technology or [sports leagues' and NCAA institutions'] adoption of new methods."[133] Some scholars argue that because the methods of collecting ABD are scientifically unproven, it is difficult to understand to what degree the data enhances future training.[134]

1. Privacy and Security Risks

Independent experts rightly forecasted that privacy issues related to wearables would "expand beyond health trackers like Fitbit and the Apple Watch to so-called smart clothing, with sensors embedded in the material itself" as a result of the amateurism debate surrounding college sports.[135] Advocates still worry legal limits and standards will fail to maintain pace with technology.[136] These concerns stem in part from hackers' motivation to access unencrypted data while in transit or storage to become privy to either the physical condition of players or teams as a whole to impact sports betting.[137] Cybercriminals are modern-day culprits, and organizations ill-equipped to guard against these security risks contribute to the danger

130. *See* McLellan et al., *supra* note 113, at 5 (noting risks unique to student-athletes); *see also* Lazzarotti et al., *supra* note 19 ("Any sports or athletic organization that develops a wearable device program, or has reason to believe that these devices are being used by coaches and others to collect similar data, should be mindful of these risks and regulatory issues.").

131. *See* Karkazis & Fishman, *supra* note 23, at 50.

132. *See* Zagger, *supra* note 23.

133. Karkazis & Fishman, *supra* note 23, at 50.

134. *See id.*

135. Tracy, *supra* note 4.

136. *See id.*

137. *See id.*

in this unmined field of privacy, "especially as the internet plays a significant role in the growing legalized sports gambling industry."[138]

2. Consent or Coercion? The Need for Informed and Meaningful Consent

NCAA student-athletes are absent from the bargaining table and even lack representation when ABD is included in vendor contracts.[139] They frequently waive ABD rights although the risks associated with unintended use are substantial.[140] Student-athlete biometric data waivers granting consent to the use of ABD fail to consider the broader ethical issues attached to ABD, such as appreciating the attendant risks associated with sharing ABD.[141] However, capitalizing on endorsement opportunities requires meaningful consent. Not only must student-athletes fully understand the scope of consent, but legislatures also must consider the power imbalance at play.

Scholars Alicia Jessop and Dr. Thomas A. Baker, III point to three contracts that control the use of student-athlete biometric data collected from wearable tracking devices: "(1) the contract between the individual school and the ABD collection device corporation, (2) the 'opt-in' agreement between the school and its NCAA athletes, and (3) terms of use agreements that NCAA athletes must consent to as a condition to use the ABD collection devices."[142] An examination of these contracts between these entities revealed that NCAA student-athletes are not parties to any of the agreements.[143] Jessop and Baker further examined whether consent could even be found in opt-in agreements or terms of use agreements accompanying the ABD collection devices.[144] Often times, the only indicator of an opt-in agreement is the student-athlete's affirmative participation in using an

---

138. Williams, *supra* note 94, at 541–42.

139. *See* Jessop & Baker, *supra* note 52, at 106 ("Unlike their professional counterparts, NCAA athletes are not represented by athlete agents or players' associations and must rely on the affirmations provided by their coaches and administrators at the institutions they choose to attend.").

140. *See id.* at 100.

141. *See* Osborne, *supra* note 10, at 73.

142. Jessop & Baker, *supra* note 52, at 100.

143. *Id.*

144. *Id.*

ABD collection device.[145] Individual NCAA programs then obtain informed consent from student-athletes agreeing to share the ABD.[146] Surprisingly, Jessop and Baker's investigation discovered only one institution that educated student-athletes of the attendant risks involved with collecting ABD.[147]

Jessop and Baker assert student-athletes lack the opportunity to give meaningful and informed consent to ensure student-athletes are actually aware of the risks assumed when opting into the use of ABD collection devices.[148] They also warn of the substantial risks accompanying data breaches and misuse of ABD identifying student-athletes.[149] As such, accountability to apprise student-athletes of risks related "with the option to participate in the use of ABD collection devices *should* be substantial."[150] To illustrate this issue, they highlight "there is no evidence that NCAA athletes are adequately informed of those risks prior to their decision to participate in the use of ABD collection devices."[151] Similarly, coaches are not trained to warn players of the risks associated with the collection and use of ABD.[152]

Based on surveying terms of agreements permitting NCAA institutions to collect, use, and disseminate student-athlete biometric data, Jessop and Baker argue the terms fail to notify student-athletes of the risks associated with exposing their ABD.[153] Additionally, their investigation of the NCAA student-athlete opt-in process revealed that NCAA institutions simply direct student-athletes to download applicable forms consenting to ABD use but fail to clarify or provide further information regarding the terms of use.[154] The imbalance of power between player and team is great, and this nonchalant manner of

145. *Id.* at 103.

146. *Id.*

147. *Id.*

148. *Id.* at 105.

149. *Id.*

150. *Id.*

151. *Id.*

152. *Id.* at 107.

153. *Id.* at 108 (explaining that "[t]he Terms of Use agreements built into applications for ABD collection devices were drafted for consumers rather than NCAA athletes").

154. *Id.*

opting in to ABD data tracking under the circumstances rings of coercion rather than meaningful consent.[155]

3. Future Earning Potential

Beyond the issue of lack of meaningful consent, "reservations lie over how ABD obtained from ABD collection devices could be used against NCAA athletes in intercollegiate athletics decisions."[156] The predictive performance value of ABD, when in the hands of a potential employing professional team, becomes a tool to access future earning potential.[157] ABD is routinely used to gauge performance primarily for future purposes.[158] Because of ABD's predictive value when it comes to productivity, sharing data without the student-athlete's consent could detrimentally affect future earning potential in professional sports.[159] Beyond ABD's potential harm to future earning potential,

---

155. *See* Jason F. Arnold & Robert M. Sade, *Wearable Technologies in Collegiate Sports: The Ethics of Collecting Biometric Data from Student-Athletes*, 17 AM. J. BIOETHICS 67, 69 (2017), https://www.researchgate.net/publication/311783654_Wearable_Technologies_in_Collegiate_Sports_The_Ethics_of_Collecting_Biometric_Data_From_Student-Athletes.

156. Jessop & Baker, *supra* note 52, at 97.

157. *See* Osborne, *supra* note 10, at 60–61.

158. *See id.* at 40.

159. *See id.* Unintended use may negatively affect future earning potential in the absence of legislation or regulations governing student-athlete biometric data. Barbara Osbourne explains the effects on student athletes:

> So far, 50 teams and 12 schools within the National Collegiate Athletic Association (NCAA) adopted the WHOOP band. And unlike the collective bargaining that happens at the professional level, there are no unions for student-athletes. These players could be forced or 'highly encouraged' to wear the band by a coach who has the power to determine if they make it to the professional level. College scouts and recruiters could misuse the data to bargain in their favor to sign players, capitalizing on their vulnerability. Data could intervene with regular college and high school life to the point where kids who want to be professionals are monitored 24 hours a day. While still figuring out their bodies and adjusting to new academic environments, there could be many data points that result in ruined careers before they [ha]ve even started.

student-athlete biometric data is also a data point in assessing scholarship renewal.[160] ABD influences how college sports programs operate, student-athletes perform, and could soon become an integral part of fan engagement, thereby providing fitting endorsement opportunities amidst the changing amateurism model in collegiate sports.

IV. WHY A BAN ON MONETIZING STUDENT-ATHLETE BIOMETRIC DATA WITHOUT MEANINGFUL PLAYER CONSENT IS PROPER

Far too many risks lie within sharing student-athlete biometric data, despite its revenue and performance potential. Presumptions of how states, courts, and the NCAA would treat student-athlete biometric data in the event a player is harmed as a result of a security breach or misuse of the information are not enough. Current biometric data privacy laws are designed to protect consumer privacy, not student-athletes. Student-athletes deserve a voice to speak on their behalf as to the manner in which their ABD data use is used and that voice is principally elected officials.

A. Protecting the Choice to Profit

The NCAA sports industry is a multi-billion-dollar market that profits annually off of the talents of student-athletes who are prohibited from receiving compensation.[161] In October 2019,

---

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

160. Zagger, *supra* note 23. Depending on the professional league, statistical data may or may not be a permissible factor to determine a player's predictive value during contractual negotiations. The NBA prohibits ABD use during contractual negotiations. *See* Osborne, *supra* note 10, at 61. MLB lists data generated through wearable technology as an "admissible statistic" during arbitration hearings. *See* BASIC AGREEMENT, *supra* note 48, at 22.

161. *'Student Athlete,' the Latest Doc from LeBron James, Examines the Exploitation of College Athletes*, THE UNDEFEATED (Oct. 2, 2018), https://theundefeated.com/features/student-athlete-hbo-documentary-from-lebron-james-examines-the-exploitation-of-college-athletes/ (concluding with Lebron James's comment that student athletes are "'propelling a billion-dollar industry and getting [a] sweatsuit for it'").

California enacted the California Fair Pay to Play Act permitting student-athlete compensation for the use of their NILs.[162] Under the bill, student-athletes can hire agents to garner sponsorship and business deals.[163] While many states are expected to follow California and enact laws similar to the Fair Pay to Play Act allowing student-athletes to profit from NIL endorsements, legislation is not in place to govern student-athlete biometric data.[164] Similarly, players must understand the risks of monetizing their ABD.[165] In the absence of a players union to advocate for the regulation of student-athlete biometric data and no NCAA policy directing the use of student-athlete biometric data, it is incumbent upon states to enact laws designed to guard against the misuse of such personal and invasive data.

Student-athletes' recently-acquired right to capitalize on the use of their NIL presents the option to monetize ABD. Given the privacy risks, a statute should also contemplate the unintended consequences of a security breach, and the misuse of data, such as hacking or sharing information with professional associations. Legislation should respond to technological advances in ABD tracking, contemplate the breadth of information biometric data captures, and provide a framework to protect uniquely identifiable information.[166] The

---

162. Charlotte Carroll, *Tracking NCAA Fair Play Legislation Across the Country*, SPORTS ILLUSTRATED (Oct. 2, 2019), https://www.si.com/college/2019/10/02/tracking-ncaa-fair-play-image-likeness-laws.

163. *See id.*

164. *See id.*; Lazzarotti et al., *supra* note 19; Zagger, s*upra* note 23. The NCAA's vote came on the heels of California's bill, and at least twenty-eight states have enacted similar bills, including: Colorado, Florida, Illinois, Kentucky, Minnesota, Nevada, New York, Pennsylvania, and South Carolina. *See* Carroll, *supra* note 162; Dellenger, *supra* note 88.

165. *See supra* Section III.C.

166. *See* Arnold & Sade, *supra* note 155, at 67–70 ("Until privacy safeguards are established by such a council, universities and the NCAA should discourage the sharing of biometric data among teams and conferences without the explicit consent of the player. Commercial use of individually identifiable biometric data collected from student-athletes should be permitted only with the athlete's permission. Further research on the validity and interpretation of biometric data in amateur and professional sports is urgently needed and should include a more systematic approach to gathering information on the prevalence of biometric technologies and on existing privacy protections.").

following model statute proposes the manner in which student-athlete biometric data should be regulated for the benefit of the developing body and player autonomy in a new age of the student-athlete's ability to profit from their NIL.[167]

This model statue directs the manner in which institutions and other entities collect, use, and store student-athlete biometric data; renders any provision or agreement purporting to waive student-athlete biometric data rights void and unenforceable; covers notice and consent; and provides a comprehensive definition for biometric data. The proposed model statute is fashioned after MLB's regulatory approach, which tracks the Illinois BIPA and currently bans any commercial use of ABD.[168] The statute also borrows language from the CCPA and additionally tracks current state legislatures' definitions of biometric data to create a uniform definition for biometric data for states to adopt in the proposed regulation of student-athlete biometric data.[169] Finally, the Fair Pay to Play Act serves as a model for the suggested statute in that it contemplates the NCAA's action to allow student-athletes to profit from their NILs.[170] This ban on monetization applies to all wearable device corporations, including Apple, Catapult, Whoop, Firstbeat, and any other ABD collection device regardless of whether the entity has a contractual agreement with an NCAA institution.

B. Applying the Solution

As applied to the fictional Asia Cummings, the legislation and regulation governing her election to monetize her data implements several requirements this Note aims to present as imperative to protect her interests as well as other NCAA student-athletes who may opt to participate in ABD collection. Prior to Asia's NCAA participation in an ABD collection program, her NCAA institution would require a training session informing Asia of the associated risks involving her

---

167. *See* Appendix A.

168. *See* BASIC AGREEMENT, *supra* note 48, at 334.

169. *See* CCPA, CIV. CODE § 1798.140(b) (West 2020) ("Biometric information includes, but is not limited to . . . gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.").

170. *See* Fair Pay to Play Act, CAL. EDUC. CODE § 67456 (West 2020) (effective Jan. 1, 2023); Appendix B.

permission to allow the NCAA, an NCAA institution, or any other entity to collect, store, and use her ABD. Administrators conducting seminars must have a reasonable understanding and be sufficiently competent to communicate the attendant risks of such a grant. Beyond informed consent, this proposed regulatory framework grants Asia control of the collection, use, and dissemination of her ABD. The NCAA institution is further prohibited from sharing her ABD metrics without Asia's consent. In addition to her consent, the legislation grants her the authority to set limits to the manner in which her ABD is used. As for security measures, this proposed legislation mandates that the participating NCAA institution and any other entity contracting to use her ABD must encrypt Asia's data to guard against hacking or any other unauthorized use.

Due to the lack of bargaining power and the infancy of student-athlete NIL endorsement rights, this Note recommends prohibiting sharing data with professional leagues or any entity with the potential to effect Asia's future professional endeavors due to its unproven validity. The NCAA and any other entity with an interest in commercializing her data would be required to obtain Asia's express consent, give an explanation of the intended use, set limits to guard against unwanted disclosure, and be subject to a complete bar on sharing the data with any agents. The participating NCAA institution must also destroy any data upon express notification of Asia's desire to no longer participate in ABD collection. Finally, if Asia learns her ABD is being used against her interest[171] or should the data usage exceed the scope of her consent, the regulation expressly provides a private cause of action against the NCAA institution.

V. CONCLUSION: PROTECTING THE DECISION BY PROHIBITING MONETIZATION WITHOUT MEANINGFUL STUDENT-ATHLETE CONSENT

The wearable technology industry is booming, as is its use in college sports. Legislation should limit the use of student-athlete biometric data among NCAA institutions for the good of the athlete in

171. *See* Lazzarotti et al., *supra* note 19 ("Teams can use the biometric data to justify cutting an athlete's playing time and, in the case of professionals, as leverage in contract negotiations. And athletes have justifiable concerns over surveillance of their activities and how their data is being stored and protected."); Zagger, *supra* note 23.

terms of player performance, injury prevention, and potential revenue reservation. While student-athletes currently consent to ABD use, they lack control of how it is collected, stored, and/or disseminated. Further, scholarship shows this consent does not sufficiently apprise students of the associated risks, of which there are many. The law is currently ill-equipped to protect student-athletes when it comes to ABD collection because current biometric privacy laws are designed to protect consumers; student-athletes lack a union to advocate for their ABD interests; and wearable ABD-tracking technology is rapidly advancing. The absence of legislation dedicated to governing student-athlete biometric data demands state action to safeguard student-athlete interests.

Student-athletes must have a *meaningful right* to opt-out of biometric tracking as well as a *meaningful right* to expressly consent to monetizing personal ABD.[172] Any third-party usage for commercial purpose agreements should be established between the athlete and the entity requesting the data and provide informed consent for the purposes of protecting private information unique to a student-athlete to guard against unforeseen consequences.[173] The NCAA is

---

172. *See* Jeremy Venook, *The Upcoming Privacy Battle over Wearables in the NBA*, THE ATLANTIC (Apr. 10, 2017), https://www.theatlantic.com/business/archive/2017/04/biometric-tracking-sports/522222/. Pursuant to the NBA's new collective-bargaining agreement, players may opt out of participating in biometric tracking. *Id.* The league prohibits use of wearables during games and the voluntary use of wearables in practice is limited to one of six brands. *Id.* Teams "requesting a player wear one must explain, in writing, what's being tracked and how the team will use the information, not only to the player himself but also to a six-person panel comprising three representatives for the players' union and three for the league." *Id.* Student-athletes deserve a similar process.

173. Osborne's discussion of the NBA CBA, which emphasizes player ownership of personal ABD, illustrates an approach to protecting ABD applicable to the college sports context:

> The NBA CBA is the first of its kind in United States professional sports to address ABD, and the result is a set of provisions largely intended to protect the players. The CBA specifies that a joint committee must set standards for device functionality and cybersecurity, and vet all wearables based on the functionality and cybersecurity standards; teams must comply with those standards; no wearables are allowed in games; players have full access to data while staff has limited access to data; wearables are voluntary; and

experiencing a new age in amateurism and with this paradigm shift comes the realization of economic opportunities the student-athlete has never encountered. Yet, with the expansion of opportunities comes the responsibility to address the risks, and without immediate legal action, student-athletes are left unprepared and unprotected when it comes to ABD collection and usage. In an ever-evolving legal and economic world, such a charge to protect begins with state legislation and internal NCAA regulation.

> teams can only use ABD for player health, performance, on-court strategy, and tactics and *not* for anything else—particularly contract negotiations, release to the public or commercial purposes; and that teams can be fined up to $250,000 for violations. The 2017 NBA CBA "establish[es] . . . a presumption that players own all data about themselves, and ban the use of wearable data in contract negotiations." Sources report that teams treat the CBA as protecting the purely permissive nature of wearables, and allowing players to make their own judgments as to whether they believe a particular device will benefit them.

Osborne, *supra* note 10, at 60–61.

APPENDIX A
PROPOSED UNIFORM ACT
BIOMETRIC DATA PRIVACY IN INTERCOLLEGIATE ATHLETICS

(a) "The [student-athlete's] welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[174]

(b) "A postsecondary educational institution shall not uphold any rule, requirement, standard, or other limitation that prevents a student of that institution participating in intercollegiate athletics from earning compensation as a result of the use of the student's [biometric data]. Earning compensation from the use of a student's [biometric data] shall not affect the student's scholarship eligibility."[175]

(c) For purposes of this title:

(1) Biometric data means information generated by automatic measurements or analysis of physiological, biological, or behavioral characteristics for the purpose of authenticating the individual that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a [student-athlete or the student-athlete's device] that captures keystroke patterns or rhythms, gait patterns or rhythms, sleep, health, or exercise data that contain identifying information. [176]

(d) "Any commercial use or exploitation of such information or data by a [postsecondary educational institution], [NCAA], or any [NCAA]-related entity or other third party is strictly prohibited."[177]

(e) An entity expressly acquiring a student-athlete's ABD for commercial purposes "[m]ust take reasonable care to guard against unauthorized access to and acquisition of" the data[178] and "destroy the

---

174. 740 ILL. COMP. STAT. 14/1-99 (2020).

175. Fair Pay to Play Act, CAL. EDUC. CODE § 67456(a)(1) (West 2020) (effective Jan. 1, 2023).

176. *See* WASH. REV. CODE § 19.375.010(1) (2020); CCPA, CAL. CIV. CODE §1798.140(b) (West 2020); COLO. REV. STAT. § 6-1-716 (1)(a) (2020); *see also* McGinley et al., *supra* note 23.

177. BASIC AGREEMENT, *supra* note 48, at 335.

178. WASH. REV. CODE § 19.375.020(4)(a) (2020); *see also* TEX. BUS. & COM. CODE ANN. § 503.001(c)(2) (West 2020) ("A person who possesses a biometric identifier of an individual that is captured for a commercial purpose . . . shall store,

biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires."[179]

(f) "Before a [student-athlete] can voluntarily agree to use a wearable technology, the [postsecondary educational institution] must first provide the [student-athlete] a written explanation of the technology being proposed, along with a list of the [postsecondary educational institution] representatives who will have access to the information and data collected, generated, stored, and/or analyzed (the 'Wearable Data')."[180]

(g) Entities collecting, using, and/or disseminating ABD are required to encrypt ABD.

(h) This act restricts:

(1) "Any provision of a contract or agreement of any kind that purports to waive or limit in any way a [student-athlete]'s rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a [student-athlete] from declining to request information from a business, declining to [opt out] of a business' sale of the [student-athlete]'s personal information, or authorizing a business to sell the [student-athlete]'s personal information after previously opting out."[181]

(2) "A waiver of these notification rights or responsibilities is void as against public policy."[182]

(3) "[An entity] possess[ing] a biometric identifier of an individual that is captured for a commercial purpose . . . [from] sell[ing], leas[ing], or otherwise disclos[ing] the biometric identifier" outside of a limited set of exceptions."[183]

---

transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other confidential information the person possesses.").

179. TEX. BUS. & COM. CODE ANN. § 503.001(c)(3) (West 2020) (includes exceptions).

180. BASIC AGREEMENT, *supra* note 48, at 334.

181. CCPA, CAL. CIV. CODE §1798.192 (West 2020).

182. COLO. REV. STAT. § 6-1-716 (2020).

183. TEX. BUS. & COM. CODE ANN. § 503.001(c)(1) (West 2020).

(i) "Any and all Wearable Data shall be treated as highly confidential at all times, including after the [student-athlete leaves postsecondary educational institution], shall not become a part of the Player's medical record, and shall not be disclosed by a [postsecondary educational institution] . . . ."[184]

(j) A violation of this act authorizes a student-athlete a private right of action.

184. BASIC AGREEMENT, *supra* note 48, at 335.

APPENDIX B
PROPOSED NCAA REGULATION

This regulation authorizes a student-athlete to contract for the sale and use of the student-athlete's ABD.

Any agreement with a third-party is separate and apart from the student-athlete's relationship with the NCAA, and the student-athlete assumes all privacy risks associated with disclosing biometric data.

The NCAA or any third-party vendor shall provide student-athletes:

(1) "the right to know what personal information large corporations are collecting about them;

(2) the right to tell businesses not to share or sell their personal information; and

(3) protections against businesses that compromise their personal information."[185]

"Any and all Wearable Data shall be treated as highly confidential at all times, including after the expiration, suspension, or termination of this Agreement, shall not become a part of the [student-athlete's] medical record, and shall not be disclosed by a [postsecondary educational institution]."[186]

"Before a [student-athlete] can voluntarily agree to use a wearable technology, the [postsecondary educational institution] must first provide the [student-athlete] a written explanation of the technology being proposed, along with a list of the [postsecondary educational institution] representatives who will have access to the information and data collected, generated, stored, and/or analyzed (the "Wearable Data")."[187]

"Any commercial use or exploitation of such information or data by a [postsecondary educational institution], [NCAA], or any [NCAA]-related entity or other third party is strictly prohibited."[188]

185. CCPA, CAL. CIV. CODE § 1798.100 (West 2020).

186. BASIC AGREEMENT, *supra* note 48, at 335.

187. *Id.*

188. *Id.*