

Benefits and Concerns Abound, Regulations Lack in Collegiate Athlete Biometric Data Collection

Chelsea Rush and Barbara Osborne

Statistical analysis has long been a staple in sports, helping teams, athletes, physicians, fans, and others understand and predict athlete performance and develop training programs. The rise of connected, wearable devices, however, has enabled the collection and analysis of unprecedented types and amounts of athlete data. Various benefits accompany this augmented data collection ability, such as the creation of robust, individualized training and recovery programs. Conversely, such substantial data collection also leads to significant concerns related to athlete privacy, misuse of data, and exploitation. While data collection is prevalent in both professional and amateur sports, this article focuses on data collection in the nuanced landscape of intercollegiate athletics. The discussion begins with an overview of the ways athlete data is collected and used, then delineates the concerns specific to intercollegiate athletics. The various existing regulatory frameworks that apply to this space are then explored to determine how, if at all, the frameworks may provide protections against the various concerns. To conclude, numerous recommendations for curing the shortcomings of these regulatory frameworks and ensuring protection of athlete interests are provided.

Keywords: athlete biometric data, athlete privacy, wearable devices, intercollegiate athletics, NCAA, Family Educational Rights and Privacy Act

Introduction

Released in 2011, the film adaptation of Michael Lewis's *Moneyball* placed sport data analytics in the public eye, demonstrating to mainstream media consumers just

Chelsea Rush is a JD candidate at the University of North Carolina School of Law. She also completed her undergraduate education at the University of North Carolina at Chapel Hill, double majoring in sport administration and communication studies. Her specific interests include legal issues in sport, intellectual property, and privacy. Email: chelsearush10@gmail.com

Barbara Osborne, JD, is a professor of sport administration in the Department of Exercise and Sport Science, with a joint appointment at the School of Law at the University of North Carolina at Chapel Hill. Her research interests include legal issues in intercollegiate athletics, women's issues in intercollegiate athletics, and medical safety issues in sport. Email: sportlaw@unc.edu



how significantly statistical analysis can affect sports.¹ Only a decade later, wearable technology² has become a multi-billion dollar industry and has exponentially increased the ability to collect data and make data-driven decisions in sports.³ With wearable devices, such as FitBits and Apple Watches, enabling collection of up to 1,000 data points per second, teams can easily synthesize massive amounts of athlete biometric data (“ABD”) to better understand player performance, tailor training programs, monitor health and wellness, and more.⁴ Collection of such vast amounts of personal data, however, comes with legal and ethical concerns, such as privacy invasion and exploitation. While ABD is attractive at both professional and amateur levels, this article focuses on the potential implications and regulatory frameworks related to the nuanced landscape of intercollegiate athletics.

The practice of data collection via wearables is still in its infancy compared to the collection and analysis of traditional sport statistics, such as batting average and free throw percentage. As such, this article does not present a chronicle of how ABD has been collected and used in intercollegiate athletics or the actual results of such collection and use. Instead, by discussing many of the possible uses and outcomes of ABD in intercollegiate athletics, as well as certain applicable regulatory frameworks, this article seeks to proactively identify potential concerns and remedies while ABD collection is still quite novel. Part I will explain what ABD is, how it is collected, and how it is used. Part II will discuss various implications and concerns raised by ABD collection in intercollegiate athletics. Part III will provide overviews of various regulatory frameworks that relate to, and may provide some basis for regulating, intercollegiate ABD collection, and Part IV will provide recommendations to assure protection of the interests discussed herein.

¹ See Dyuti Lal, *Moneyball The Must Watch Movie: Key Learnings for Every Aspiring Data Analyst and Data Scientist*, MEDIUM (Nov. 13, 2019), <https://medium.com/@dyutilal/moneyball-the-must-watch-movie-key-learnings-for-every-aspiring-data-analyst-and-data-scientist-756690e45aa3> [<https://perma.cc/A488-7PQL>].

² The terms “wearable technology,” “wearable devices,” “wearables,” “smart devices,” and “connected devices” are used throughout this article to refer to devices that track data related to performance, movement, and health and are worn on the body or used in training or competition, such as sensor-equipped garments, helmets, bats, etc.

³ 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, 67-68 (2017).

⁴ See Barbara Osborne & Jennie L. Cunningham, *Legal and Ethical Implications of Athletes’ Biometric Data Collection in Professional Sport*, 28 MARQ. SPORTS L. REV. 37, 38-45 (2017).



Part I: ABD and Wearable Technology Explained

Biometrics in sport generally refers to the “measurement and tracking of physical and physiological characteristics [of athletes] for the purpose of assessing performance and recovery.”⁵ ABD can include biomechanical measurements of muscular and skeletal movement and impact; physiological measurements, such as hydration levels, temperature, and heart rate; or behavioral measurements, such as sleep patterns.⁶ With wearables and other smart devices, the types and amount of data that can be collected are nearly endless, and monitoring of certain characteristics can occur around the clock.⁷ Coaches and others have traditionally collected data by relying on medical examinations and by observing, measuring, and calculating results of various drills and exercises.⁸ However, now, connected devices allow for monitoring of various characteristics throughout practices, in game situations, and away from the field. For example, prior to the fall of 2020, the University of Tennessee outfitted its entire athletic department with WHOOP wristbands. The devices were said to allow teams to continuously monitor their student-athletes’ physiological data to gain “insights into early warning signs” of illness, in light of the COVID-19 virus.⁹

The WHOOP wristband is touted by the company as a “performance optimization system.” It measures and analyzes key metrics, including heart rate, ambient temperature, sleep, and other information, to provide insights on strain and recovery, predict performance based on those insights, and guide performance improvements through training and behavioral modifications.¹⁰ While devices like the WHOOP wristband are worn continuously for optimal results about overall wellness, strain, and recovery, other wearables, like smart clothing or harnesses, may be used only during training or specific activities.¹¹ Such devices may be sport-specific or sport-neutral. For example, in baseball, sensors in

⁵ Katrina Karkazis & Jennifer R. Fishman, *Tracking U.S. Professional Athletes: The Ethics of Biometric Technologies*, 17 AM. J. BIOETHICS 45, 46 (2017).

⁶ See Osborne & Cunningham, *supra* note 4, at 38.

⁷ See *id.* at 38-44 (listing various ABD devices, such as clothing, wristbands, bandages, helmets, bats, and other equipment and the types of data they are used to track and synthesize).

⁸ See Karkazis & Fishman, *supra* note 5, at 45.

⁹ Kristen Holmes, *WHOOP to Be Worn by All University of Tennessee Athletes*, WHOOP, <https://www.whoop.com/thelocker/whoop-on-university-of-tennessee-athletics/> (last visited October 27, 2021) [<https://perma.cc/6P4B-5TAU>].

¹⁰ Osborne & Cunningham, *supra* note 4, at 43-44.

¹¹ *Id.* at 41-44.



bats can be used to analyze players' swings and sensors in compression sleeves can be used to analyze workload and strain on pitchers' throwing arms.¹² Other devices use similar micro-movement measurements to demonstrate whether athletes favor one side or other, whether movement patterns are consistent, and how explosive and efficient movements are, to determine if muscular imbalances exist, if injury is likely to happen, etc.¹³

Devices generally send data to the tracking system provided by the maker of the device, where the data is analyzed and stored, then insights are reported via the dashboard made available to the team through applications or other web-based platforms.¹⁴ Some devices require that athletes download applications onto their own phones and connect their phones to the devices.¹⁵ Those devices send data to the athletes' phones, which then transmit data to the central system that analyzes and stores the teams' data.¹⁶ Some ABD systems may only provide team insights to designated personnel, while some may provide various team analytics to anyone connected to the team's platform or accounts.¹⁷

ABD can be manipulated and analyzed to reveal insights about athlete health, stress, and recovery, helping teams focus on overall health optimization and build more effective training regimens and injury rehabilitation programs.¹⁸ Data can also be used to optimize sport-specific movement patterns and performance.¹⁹ Behavioral tendencies, location information, and physiological indicators can also be revealed through data collection.²⁰ Such insights can be used to make determinations about athletes' personal decisions and whether they are taking care of themselves away from their training facilities, which could then be used in decisions about disciplinary action or modified playing time.²¹

While ABD reveals a great deal of performance and health-based insights of interest to both athletics programs and athletes, many third parties also have

¹² *Id.* at 42-43.

¹³ *Id.* at 41-44.

¹⁴ See 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, 88-97 (2019); Karkazis & Fishman, *supra* note 5, at 47-48.

¹⁵ *E.g.*, Karkazis & Fishman, *supra* note 4, at 47-48; *Experience*, WHOOP, <https://www.whoop.com/experience/> [<https://perma.cc/VA62-NURP>] (last visited Nov. 29, 2020).

¹⁶ *E.g.*, Karkazis & Fishman, *supra* note 5, at 47-48; *Experience*, WHOOP, <https://www.whoop.com/experience/> [<https://perma.cc/VA62-NURP>] (last visited Nov. 29, 2020).

¹⁷ Karkazis & Fishman, *supra* note 5, at 53.

¹⁸ Osborne & Cunningham, *supra* note 4, at 45-46.

¹⁹ *Id.*

²⁰ Karkazis & Fishman, *supra* note 5, at 50-51.

²¹ *Id.*



interests in ABD, leading to its commercialization.²² Fans, fantasy sport enthusiasts, and gamblers, for example, revel in having extensive knowledge about athletes.²³ Producers of sports content and broadcasts, thus, are equally interested in access to ABD to enable them to provide additional statistics and insights that fans desire.²⁴ Finally, sporting goods makers and ABD service providers—companies who provide wearable devices or related analytics services—can utilize ABD insights to produce higher quality performance gear and services and to more effectively market their products.²⁵ For example, a sports equipment company can use ABD insights to develop equipment that is more effectively tailored to the needs of athletes. Further, a company like WHOOP can use ABD insights to continue enhancing the features and performance of its devices.

Part II: Concerns Raised by ABD Collection

Various parties hold different interests in ABD. While health and performance optimization are certainly interests held by student-athletes, their coaches, and other institutional representatives, a divergence in interests can be surmised when considering surveillance-like tracking of athletes in their down time. Athletes, on one hand, have an interest in privacy and freedom to make personal decisions, while coaches and other institutional personnel have interests in ensuring athletes are making the “right” decisions away from the field. Third parties have interests that may be completely different from those held by athletes and their institutions, as, for example, commercial entities may use ABD to increase consumption and profits and fans may use data for insights to place bets. These various interests, though sometimes aligned, form much of the basis for the concerns raised in the following discussion.

Privacy and Security

Traditional sport statistics like free throw percentage and batting average are publicly accessible, as they are generated from merely watching competition and calculating performance metrics. ABD, on the other hand, is generally innately

²² See, e.g., David W. Sussman & Amy Edgerton-Wiley, *Is Betting on an Athlete’s Heart Rate Coming to Broadcasting?*, HOLLYWOOD REPORTER (July 18, 2020), <https://www.hollywoodreporter.com/thr-esq/is-betting-an-athletes-heart-rate-a-game-coming-broadcasting-guest-column-1303582> [<https://perma.cc/7KSX-C6V3>].

²³ See *id.*

²⁴ See *id.*

²⁵ See *id.*



private information.²⁶ The methods of ABD collection, alone, are fairly privacy intrusive, as they require smart devices to be worn, placed on the body, or used by the athlete in training or competition to measure physiological or biomechanical indicators that cannot be discerned by the naked eye. The analytics revealed by such collection further encroach on privacy as they can provide revelations about health that are often reserved to care provider-patient relationships, about personal decisions and associations, and about other deeply personal attributes that are only shared with those whom athletes choose.²⁷

Coaches, athletics programs, and institutions want to utilize ABD to better understand student-athletes' performance and to ensure student-athletes remain healthy. They may also use ABD to ensure student-athletes remain eligible for competition and compliant with applicable rules and policies by monitoring athletes' "off-field" behaviors. These are interests that are generally favorable to and shared by athletes; however, athletes also face a countervailing interest in maintaining bodily integrity and decisional freedom.²⁸ ABD collection removes an athlete's privacy in her bodily movements, functions, and ailments that she otherwise may have chosen to keep private, as well as significantly diminishes her real or perceived freedom to make decisions.²⁹ For example, where a team utilizes 24-hour monitoring devices, a student-athlete may fear her choice to engage in a sexual relationship or to go certain places will be revealed to coaches, other personnel, or teammates, causing her not to move about and make decisions freely. ABD systems that allow anyone on the team's platform or account to view all data related to the team raise further privacy concerns, as all teammates, coaching staff, and personnel can see each student-athlete's data and related insights.³⁰

Similarly, third parties have interests in ABD that are sometimes favorable to athletes but that can easily run afoul from athletes' privacy interests. As evidenced in part by the number of subscription services that give fans access to sport statistics and analysis³¹ and by the body of case law around information

²⁶ Stephanie Weissenburger, *As Biometric Data Collection Increases, So Do Athletes' Concerns*, FULL COURT PRESS LEGAL (May 26, 2020), <https://www.fullcourtpresslegal.com/post/as-biometric-data-collection-increases-so-do-athletes-concerns> [<https://perma.cc/MK24-8K28>].

²⁷ See Jessop & Baker, *supra* note 14, at 96-97; Karkazis & Fishman, *supra* note 5, at 50-51.

²⁸ Karkazis & Fishman, *supra* note 5, at 57.

²⁹ See *id.*

³⁰ See Jessop & Baker, *supra* note 14, at 96-97 (discussing University of Tennessee swim team athletes' ability to view each others' data on the team's WHOOP platform).

³¹ See, e.g., *The Most Powerful Research Tools in Sports*, STATHEAD, <https://www.stathead.com/> (last visited October 20, 2021); Elite Data Analytics for Fantasy Sports Players and Next Level Fans, Synergy Sports, <https://www.synergysports.com/solutions/fans/> (last visited October 20, 2021).



requests about athletes by media, fans and media outlets alike will go to great lengths to obtain information on athletes.³² While media outlets want information that leads to engagement-generating stories, fans want the information to feel more connected with their teams, to better understand and predict performance of the athletes they watch, to place more informed bets, etc.³³ Providing certain ABD to third parties, for these reasons, can be favorable to student-athletes, as it may lead to more coverage of their sports and potentially generate more fame and notoriety for them personally. However, third parties do not only desire information that reflects positively on athletes or that athletes would always willingly share, which is where their interests diverge from the privacy interests of student-athletes. For instance, ABD may reveal health issues student-athletes have an interest in keeping out of the public eye in order to avoid negative attention or misunderstanding of the issue's origin or severity.

Student-athlete privacy is a concept that has been addressed by courts in the context of drug testing. Courts have generally held that mandatory drug testing does not violate student-athlete privacy rights, as athletes have a diminished expectation of privacy, as compared to a general student body, due to the communal and physical nature of athletics.³⁴ However, in these cases the diminished expectation of privacy is addressed only as it relates to the relationship between athletes and their institutions and to single instances of intrusion, rather than programmatic, continuous monitoring. ABD programs and their related privacy concerns, thus, can be distinguished from the drug testing cases and their related principles. When completed continuously and not limited to very specific metrics, ABD collection can be considerably more invasive than drug testing. Drug testing happens in a single instance on a random or periodic basis and can only reveal certain medical issues. In contrast, ABD collection can produce millions of data points and innumerable insights related to an athlete. Further, where third-party sharing is contemplated in ABD programs, the examination of reasonable expectation of privacy is no longer limited to the relationship between the student-athlete and their institution. As such, cases that have addressed athlete privacy provide some basis for considering the level of privacy

32 See, e.g., *Kirwan v. The Diamondback*, 352 Md. 74 (Md. 1998) (campus newspaper brought suit under Maryland Public Information Act to compel disclosure of student-athletes' campus parking ticket records); *Nat'l Collegiate Athletic Ass'n v. Associated Press*, 18 So. 3d 1201 (Fla. Dist. Ct. App. 2009) (news organizations brought suit under public records law seeking disclosure by the NCAA of information related to dispute resolution and disciplinary proceedings); See also Karkazis & Fishman, *supra* note 5, at 53-53 (discussing the particular likelihood of hacking to obtain athlete data).

33 Sussman & Edgerton-Wiley, *supra* note 22.

34 See *Bd. of Ed. of Indep. Sch. Dist. v. Earls*, 122 S.Ct 2559, 2566 (2002); *Hill v. Nat'l Collegiate Athletic Ass'n*, 865 P.2d 633, 9 (Cal. 1994).



student-athletes can expect; however, they should not be viewed as reason to disregard the privacy concerns raised by ABD collection.

De-identification of ABD is one method for attempting to protect privacy interests.³⁵ Data that is shared in aggregate and does not identify individuals may, in fact, prevent student-athletes from being subjected to unreasonable privacy intrusions; however, ABD is arguably most valuable to and sought after by third parties when it is related to specific athletes.³⁶ Further, because those involved in intercollegiate athletics represent a small percentage of the population and individual athletics teams represent an even smaller subset, practitioners argue that re-identification of ABD from aggregated data sets likely would not prove extremely difficult.³⁷

As ABD collection and use can lead to significant intrusions into student-athletes' privacy, security of ABD is a further concern. Significant banks of data stored on physical and cloud-based servers create risks of hacking and breaches.³⁸ The most renowned student-athletes and those who play revenue-generating sports, like basketball and football, are likely the most at risk for having their deeply personal information individually sought and shared publicly. Due to their positions of notoriety, those student-athletes' information is generally of most interest to sport consumers and to commercial and media entities who profit from sport consumption. However, all student-athletes' privacy is at risk where a data breach could reveal banks of ABD.³⁹ While de-identifying ABD can provide some protection in the case of a breach, as already discussed briefly, in subsets of data like ABD, re-identification remains a legitimate concern. Because ABD programs⁴⁰ are generally administered through third-party companies that provide devices, analytics, and storage, the security of ABD is largely based on their privacy and security protocols and their contractual agreements with institutions.⁴¹ Even if ABD is stored by collegiate institutions on their own servers,

³⁵ See Karkazis & Fishman, *supra* note 5, at 51.

³⁶ See *id.*

³⁷ Osborne & Cunningham, *supra* note 5, at 72, 83.

³⁸ Karkazis & Fishman, *supra* note 5, at 53-54.

³⁹ Gilbert Smolenski, *When the Collection of Biometric and Performance Data on College Athletes Goes Too Far*, 54 WAKE FOREST L. REV. 279, 295 (2019).

⁴⁰ The phrase "ABD programs" is used throughout this article to generally refer to institutions' collection and use of ABD within their athletics programs.

⁴¹ See *id.*



the data passes through the devices and analytics platforms provided by the ABD companies, making security of ABD necessarily a joint effort.⁴²

Due to the personal nature of ABD, student-athletes have a significant and understandable interest in privacy of such data, and those interests are met with insatiable appetites from various parties for access to the data. Thus, ABD programs should address this privacy interest with measures that ensure student-athletes do not face unreasonable and unnecessary intrusions and that ABD storage and access to ABD is adequately secure. Because colleges regularly deal with student records, they likely are familiar with certain data protections. However, the nuanced, highly sensitive, and sought-after nature of ABD raises questions about whether schools and athletic departments are sufficiently equipped and educated to properly manage the data as well as concerns of when data tracking grows into unreasonable surveillance.⁴³ Further, athletics departments are no strangers to contracting with third parties for various services and sponsorships, but those contracts have only just begun to address ABD collection or sharing.⁴⁴ This raises concerns about whether athletics departments fully understand the privacy implications at stake, how to safeguard them, and what to require of ABD service providers to protect student-athletes' interests.

Misinterpretation and Negative Use of ABD

While ABD provides insights allowing for implementation of more effective training and health management, potential for negative or abusive practices also exists. In professional sports, players naturally fear ABD insights will be utilized by teams in contract negotiations, leading to loss of income or career opportunities.⁴⁵ By relying on insights they may otherwise have no way of obtaining, such as certain health or behavioral information, teams may gain bargaining leverage over athletes.⁴⁶ As amateurs, collegiate athletes do not negotiate contracts and salaries with their institutions, but they have comparable

⁴² As mentioned in the introduction, this article does not purport to analyze the ABD and contracting practices of collegiate athletic programs as they currently stand, but instead, gives a broad overview of this space and the potential implications of ABD collection and use. Thus, how institutions and ABD service providers have actually partnered to secure data is outside the scope of this article. Such research, through information requests and interviews, would, however, prove a worthy exercise in the near future as an increasing number of institutions begin to rely on ABD.

⁴³ See Jessop & Baker, *supra* note 14, at 94-99.

⁴⁴ *Id.* at 82-83.

⁴⁵ Osborne & Cunningham, *supra* note 4, at 65-68.

⁴⁶ See *id.*



concerns around the effects of ABD on scholarship opportunities and future draft and earning potential, as performance and behavioral information related to ABD could damage their reputation or profile as an athletic prospect.⁴⁷

Twenty-four-hour tracking provides schools and coaches data to better serve the health and well-being of student-athletes, but such surveillance-like tracking also creates opportunities for abusive control.⁴⁸ Consider an athlete wearing a device continuously for the purpose of tracking overall health and recovery. Data about that athlete's sleep, heart rate, body temperature, and other elements are understandably important for analyzing health and developing training and recovery programs. However, coaches having access to data that reveals that athlete's location and movements away from the field can become problematic. On one hand, unreasonable expectations, and associated punishments, related to the athlete's off-field choices, such as limitations on when and where the athlete may travel, may be set. On the other hand, insights into the athlete's lifestyle may create biases that lead to discrimination or differential treatment where the athlete's (actual or perceived) lifestyle diverges from the lifestyle choices approved of by the coaches. This control may also be exerted over different players in different ways, as certain athletes may be placed under greater scrutiny than others. Athletes of color and LGBTQ athletes have historically been subjected to differential treatment,⁴⁹ for example, and insights into personal lives or the ability to scrutinize behavior using ABD could lead to further abuses.⁵⁰ Consider that the athlete in the previous example is a gay woman whose coach harbors implicit or explicit biases against homosexuality. That athlete may find herself subjected to more strict off-field expectations and monitoring than her teammates—expectations and monitoring that effectively limit her ability to move about and engage in relationships she chooses.

Student-athletes who have an interest in competing beyond college may face issues of having their sensitive data accessed and used against them by professional recruiters or other entities.⁵¹ Such access may, for example, come by way of data leaks or through communication with team personnel, whether or not such communication follows proper protocol. While only a small population of student-athletes face concerns over future earning potential being affected by ABD, many more face concerns about scholarship renewal (for those on athletic

⁴⁷ See Jessop & Baker, *supra* note 14, at 94-99.

⁴⁸ Smolenski, *supra* note 39, at 295-96.

⁴⁹ Matthew J. Mitten et al., *SPORTS LAW AND REGULATION* 699-702, 844-858 (Wolters Kluwer, 5th ed. 2020).

⁵⁰ See Karkazis & Fishman, *supra* note 5, at 55.

⁵¹ Jessop & Baker, *supra* note 14, at 99.



scholarship) or simply having a place on the team (for those without athletic scholarships).⁵²

Misinterpretation of data or blind reliance on data may also lead to negative outcomes for teams, institutions, and student-athletes, alike.⁵³ An attractive feature of ABD is its objectivity. Theoretically, ABD provides objective measurements of exertion, recovery, and more, eliminating the need for subjective assessments of perceived strain, effort, and capacity.⁵⁴ Reliance on completely objective data, however, can lead to erroneous conclusions about student-athletes' health, exertion, or behavior.⁵⁵ For instance, where a student-athlete's ABD analysis indicates injury recovery should be complete, but the athlete is still not performing at pre-injury performance levels and sleep patterns appear poor, a coach may rely solely on the data at hand to conclude the student-athlete is prioritizing social life and not exerting their best efforts, or has not seriously engaged with the recovery plan. The student-athlete may, however, be losing sleep and underperforming due to chronic anxiety about the injury—anxiety the athlete has hidden to avoid mental health stigma. Further, effective ABD utilization depends on accurate data and accurate assessment of data.⁵⁶ Therefore, incorrect data or incorrectly interpreted data can result in student-athletes being overworked or improperly rehabbed from injury or in having reputation-damaging conclusions drawn about them.⁵⁷ Consider further the athlete in the aforementioned example who is recovering from injury. The analysis that was completed immediately after the athlete's injury may have depended on measurements from a connected device that were misinterpreted by team staff. That misinterpretation resulted in an erroneous baseline from which the athlete's recovery program was developed. When the recovery program proved under-effective, not only was the athlete's own health negatively affected, but so too could be the athlete's reputation as a dedicated, hard-working team player.

The potential for misinterpretation, abuse, and other negative outcomes of ABD collection is significant. Wearable devices can provide not only particularized training and performance insights, but also the ability to surveil, and effectively control, off-field choices and behaviors. Further, ABD is generally quite nuanced, technical information that is more likely to be misinterpreted and misused than are more traditional sport statistics. These points raise concerns

⁵² *Id.*

⁵³ *Id.* at 94-96.

⁵⁴ See Karkazis & Fishman, *supra* note 5, at 48, 55.

⁵⁵ *Id.* at 48.

⁵⁶ Jessop & Baker, *supra* note 14, at 94-96.

⁵⁷ *Id.* at 94-99.



about whether coaches, athletics personnel, and other institutional representatives are adequately educated in how to properly use and understand ABD and whether effective safeguards exist to protect student-athletes from abusive control and treatment.

Commercialization and Exploitation

Various parties other than teams and players have interests in ABD, resulting in the data being a potentially lucrative revenue stream.⁵⁸ For example, the University of Michigan recently signed a nearly \$174 million contract enabling Nike to utilize ABD of student-athletes collected via smart garments and equipment provided by the brand.⁵⁹ Undoubtedly, producers of sporting goods, and other entities that can use ABD to enhance their production of goods, services, or content, will continue lining up to pay significant sums for access to collegiate ABD, especially if they cannot gain similar access to professional athlete data due to collective bargaining agreements.⁶⁰ Further, sport gambling is a growing industry segment, and access to further data, such as players' heart rates or other physiological indicators during big moments of games, could stimulate further gambling.⁶¹ ABD not only could give gamblers more information upon which to make decisions, but could also simply create new categories of information upon which bets are placed. Similarly, fantasy sport enthusiasts, whether actively betting on their fantasy teams or not, could also use ABD to make more informed roster decisions.⁶² Due to sport consumers' appetite for information, broadcasting entities would also enjoy access to ABD in order to increase viewership and fan engagement.⁶³ Consequently, the practice of institutions licensing ABD or selling ABD rights is likely to continue growing.

Third-party interest in ABD can be favorable to student-athletes and their institutions, as it can increase exposure of athletes and their programs and can provide sport consumers with more personal information about athletes. Thus, both the notoriety of athletes and the attachment fans feel to them can be enhanced. However, commercial interests also raise significant concerns of student-athlete exploitation. To ensure the education of student-athletes is prioritized, an underlying tenet of the National Collegiate Athletic Association ("NCAA") regulatory framework is the protection of athletes as students first and

58 See, e.g., Sussman & Edgerton-Wiley, *supra* note 22.

59 Jessop & Baker, *supra* note 14, at 82-83.

60 See *infra* Part III.

61 Sussman & Edgerton-Wiley, *supra* note 22.

62 Karkazis & Fishman, *supra* note 5, at 54.

63 Sussman & Edgerton-Wiley, *supra* note 22.



avoidance of exploitation of them as athletes.⁶⁴ Agreements between colleges and commercial entities that directly implicate student-athletes through the sale and third-party use of their personal data raise concerns of this type of exploitation. Where their institutions negotiate agreements with third parties, student-athletes will likely feel compelled to provide any requested consent around disclosure of their data,⁶⁵ discussed further *infra*, and they are not involved in negotiation of such agreements.⁶⁶ This creates a situation in which student-athlete personal data can be exploited for financial gain of the institution without the athletes having a voice in the negotiation or benefitting directly from the gains.⁶⁷ The increasing commercialization of ABD raises concerns about whether regulations are in place to ensure student-athletes are not subjected to unreasonable exploitation and whether the parties negotiating deals for data rights are adequately considering the interests of student-athletes to ensure they are not subjected to unreasonable exploitation.

Consent and Coercion

Regulations on data collection and sharing often depend on consent—as long as consent is received, collected data can be disseminated to others.⁶⁸ This is a tenet that institutions will likely rely on to justify their collection of ABD and their sharing of the data with ABD service providers and other commercial entities, as student-athletes are likely to provide any consent requested by their institutions.⁶⁹ Provision of such consent, however, raises several concerns.

First, student-athletes may not be truly informed about what their consent authorizes. Evidence has shown that many institutions use informal “opt in” practices, such that consent is assumed when student-athletes use ABD collection devices provided by their programs.⁷⁰ Institutions also have a reputation for administering student-athlete contracts by “herd[ing athletes] into a room” and

⁶⁴ NAT'L COLLEGIATE ATHLETIC ASS'N, DIVISION I MANUAL 3 (2020), <https://web3.ncaa.org/lstdbi/reports/getReport/90008> [<https://perma.cc/QCN5-L4KM>].

⁶⁵ Smolenski, *supra* note 39, at 59.

⁶⁶ Jessop & Baker, *supra* note 14, at 91-94.

⁶⁷ Since this article was written, significant changes in NCAA regulation occurred, allowing student-athletes to profit from their name, image, and likeness (“NIL”) through personal endorsement deals. While student-athletes may individually engage in deals whereby they allow entities to collect and use their ABD, those deals do not change the fact that athletics programs engage in contracts that enable entities to use student-athlete ABD and that those agreements (1) are negotiated without student-athletes at the bargaining table and (2) only financially benefit the institutions. This is discussed further in Part III *infra*.

⁶⁸ See e.g. 20 U.S.C. § 1232g.

⁶⁹ See Smolenski, *supra* note 39, at 293-94; Jessop & Baker, *supra* note 14, at 104-107.

⁷⁰ Jessop & Baker, *supra* note 14, at 103-04.



having them sign forms with little information or discussion on the content or implications of the contracts.⁷¹ Where consent is obtained in those ways, prior to their ABD device use, student-athletes are likely not informed what the collection of their data will entail, who may have access to their data, and of the risks of such collection and sharing.⁷² Even where student-athletes are provided an opportunity to provide consent prior to use, evidence shows that they are not provided information about the risks they assume by participating in such programs.⁷³ Student-athletes are also, unlike professional athletes, not represented by counsel that can advise them on the balance of benefits versus risks of participating in ABD collection programs.⁷⁴

Second, student-athletes may not be given a meaningful opportunity to refuse consent. Power imbalances between student-athletes and their institutions as well as team dynamics may mean student-athletes do not feel they have legitimate opportunities to refuse consent.⁷⁵ Coaches wield a great deal of power with the ability to minimize playing time, penalize behavior, and drive the culture and community of their teams. Student-athletes, on the other hand, have no real bargaining power, as their only options are to comply with coaches' wishes, quit playing, or seek to transfer in the following season. Thus, where student-athletes are asked to provide consent to ABD collection, they are likely to feel that consent is required to ensure they are not treated differently than other members of the team.⁷⁶ Perceived pressure to consent may exist solely based on the inherent power differential or may be based on coaches' overt communication that consent is expected.⁷⁷ Team dynamics can also create coercive effects. For example, non-participation in certain team initiatives, such as use of ABD devices, by a player can lead to differential treatment by other players. On the other hand, marquee players may be able to abstain without fear of penalty, while lower ranking players may feel pressure to participate to try to earn the favor of coaches.⁷⁸

While institutions may base their authority to engage in ABD programs on the consent of student-athletes, the legitimacy of that consent is of great concern. This raises questions about whether institutions should follow certain standards when gaining student-athlete consent to ABD collection and, further, whether

⁷¹ *Id.* at 111.

⁷² *Id.* at 104-07.

⁷³ *Id.*

⁷⁴ *Id.* at 106.

⁷⁵ Smolenski, *supra* note 39, at 293-94; Arnold & Sade, *supra* note 3, at 69.

⁷⁶ See Karkazis & Fishman, *supra* note 5, at 56.

⁷⁷ See Jessop & Baker, *supra* note 14, at 104-05.

⁷⁸ Karkazis & Fishman, *supra* note 5, at 56.



coaches and other personnel are sufficiently educated on the risks of ABD programs to ensure athletes are informed.⁷⁹

Part III: Regulatory Frameworks

To properly address the concerns raised in Part II, regulation of ABD collection should address security of ABD transmission and storage, who can access the data, whether the data can be shared with third parties, and how the data can and cannot be used, among other things. However, no comprehensive, generally applicable statutory framework regulates biometric data in the United States, as the Global Data Protection Regulation does in the European Union,⁸⁰ and no industry-specific regulations explicitly address ownership, rights, and use of ABD. Therefore, ABD collection is subject to an amalgam of regulatory approaches. First, this section will outline the ways ABD is approached and regulated in professional sports to demonstrate differences in the collegiate landscape. Next, various regulatory frameworks will be discussed to demonstrate their application to ABD collection.

Collective Bargaining and Contracting in Professional Sport

Today, all major North American sports utilize some form of wearables or connected devices in training or competition, and professional athletes have serious concerns related to ABD collection.⁸¹ Professional athletes differ from student-athletes, though, as they are employees that can utilize certain tools to attempt to protect their interests.⁸² First, professional athletes in team sports have the ability to unionize into players' associations and to engage in collective bargaining.⁸³ Players' associations represent the collective interests of athletes and negotiate with league management to develop collective bargaining agreements ("CBAs") that apply to all player contracts within their respective leagues.⁸⁴ CBAs hold significant potential as an avenue for protecting player rights pertaining to ABD, as their terms govern the employment relationship between athlete and team, thus alleviating athletes from the necessity of individually negotiating for

⁷⁹ See Jessop & Baker, *supra* note 14, at 106-07.

⁸⁰ Biometric Data and Data Protection Regulations (GDPR and CCPA), Thales Group, <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data> [<https://perma.cc/UH7L-LXWG>] (last updated Nov 4, 2020).

⁸¹ Karkazis & Fishman, *supra* note 5, at 45-46.

⁸² See Osborne & Cunningham, *supra* note 4, at 57-68.

⁸³ *Id.* at 58-64. Note that not all professional leagues have unions associated with them, even where unionization is available to the athletes, and athletes in individual, rather than team, sports functionally cannot unionize, as they are not employees of a league.

⁸⁴ *Id.* at 59.



certain rights and terms of employment.⁸⁵ For example, through the 2020 National Football League (“NFL”) CBA, players were able to secure ownership rights in data collected via any sensor-based devices.⁸⁶ The CBA authorizes the NFL to use the data for certain commercial purposes, but the agreement also ensures that players share in the revenue of such use, are able to control data use beyond CBA-authorized uses, and retain the right to review additional data collection practices before they are utilized.⁸⁷ Though players retain ownership of their data, they are not able to capitalize commercially on ABD collected by devices used by their teams.⁸⁸ The agreement also specifies that, while each player’s ABD is accessible by his team’s staff, it may not be used in contract negotiations.⁸⁹ Finally, the NFL CBA, similar to the 2017 National Basketball Association CBA, created a committee to review ABD devices, uses, and practices.⁹⁰ The purpose of the committees is to ensure privacy interests are upheld, security measures are sufficient, and no inappropriate exploitation occurs.⁹¹

Second, professional athletes engage in individual contract negotiations with their teams, in which they are usually represented by experienced counsel. Through these negotiations, professional athletes attempt to leverage their potential, skills, fame, and other attributes to secure favorable salaries and employment terms, which may include securing rights in ABD, where CBAs do not address such (or where a CBA does not govern the employment relationship). While professional athletes do have access to counsel, the professional sport landscape, including the extensive control exercised by leagues and the general replaceability of athletes, results in athletes individually having minimal bargaining power in certain matters, making collective action an important means for securing rights.⁹²

In contrast, collegiate athletes have consistently been denied status as employees of their schools and of the NCAA.⁹³ Attempts of student-athletes to unionize have also been unsuccessful.⁹⁴ Thus, student-athletes do not enjoy the

⁸⁵ *Id.*

⁸⁶ NFL & NFLPA, COLLECTIVE BARGAINING AGREEMENT 295 (2020) [hereinafter NFL CBA].

⁸⁷ *Id.* at 291-95.

⁸⁸ *Id.* at 295.

⁸⁹ *Id.*

⁹⁰ NFL CBA, *supra* note 86, at 292; Osborne & Cunningham, *supra* note 4, at 60.

⁹¹ NFL CBA, *supra* note 86, at 292; Osborne & Cunningham, *supra* note 4, at 60.

⁹² *See generally* Osborne & Cunningham, *supra* note 4, at 58-68 (describing the unique structure of professional sports related to employment, collective bargaining, and individual negotiation).

⁹³ *E.g., Waldrep v. Tex. Emp’rs Ins. Ass’n*, 21 S.W.3d 692 (Tex. App. 2000).

⁹⁴ Northwestern Univ., 362 N.L.R.B. 1350 (2015).



benefits of union representation and collective bargaining to attempt to secure rights related to ABD and are, further, unable to contractually bargain with their institutions for individual rights. Consequently, student-athletes must rely on non-employment-based regulatory frameworks and the standards of their own institutions for rights and protections related to ABD collection.

NCAA Regulations

The NCAA is the largest intercollegiate athletics association and closely regulates intercollegiate sport administration for the more than 1,000 schools in its membership,⁹⁵ however, the association currently does not address ABD in its bylaws and has largely left rules for wearables up to individual sport committees and universities.⁹⁶ While this allows schools freedom to engage in ABD programs, caution should be exercised in monetizing ABD, as an institution's sale of individual student-athlete data could implicate the NCAA's amateurism and commercial exploitation tenets.⁹⁷ Similarly, NCAA regulations on scholarship non-renewals also provide some limitation on potentially negative use of ABD.⁹⁸

Bylaw 2.9 addresses amateurism, stating, "Student-athletes shall be amateurs in an intercollegiate sport, and their participation should be motivated primarily by education and by the physical, mental and social benefits to be derived. Student participation in intercollegiate athletics is an avocation, and student-athletes should be protected from exploitation by professional and commercial enterprises."⁹⁹ This provision aligns with the NCAA's commitments to protecting the integrity and competition of intercollegiate sport, ensuring education remains at the forefront for student-athletes, and safeguarding the physical and mental well-being of student-athletes.¹⁰⁰

Where student-athletes are subjected to data collection via wearable devices, the NCAA's exploitation concerns can be easily implicated. On one hand, where ABD services providers are authorized to utilize data in exchange for provision of the devices or data services, inherently intimate characteristics of

⁹⁵ See William A. Kaplin et al., *THE LAW OF HIGHER EDUCATION* 893-94 (Jossey-Bass, 6th ed. 2020).

⁹⁶ Sussman & Edgerton-Wiley, *supra* note 22.

⁹⁷ See NAT'L COLLEGIATE ATHLETIC ASS'N, *supra* note 64, at 3.

⁹⁸ See *id.* at 215-219.

⁹⁹ See *id.* at 3. Note that with the changing landscape of NIL regulation, this rule will likely evolve. However, guarding against exploitation of student-athletes seems likely to remain a fundamental tenet of the NCAA's governance.

¹⁰⁰ See *id.* at xiii.



the student-athletes are being exploited for services used to increase athletic programs' performance standards.¹⁰¹ Where institutions go so far as selling rights to ABD for profit, exploitation is clear, given that student-athletes are not involved in those negotiations.¹⁰² While student-athletes may consent to ABD practices, the NCAA's exploitation principles are nonetheless implicated, in part due to the questionable adequacy of consent, as previously discussed. Additional guidance from the NCAA is needed to give institutions notice of what, exactly, constitutes impermissible exploitation related to commercialization of ABD.

The NCAA's amateurism ideal has been a significantly contested principle whereby student-athletes could not be paid to play or paid for their likeness as athletes.¹⁰³ While student-athletes still cannot be paid to play their sports, as of July 1, 2021, the NCAA began allowing student-athletes to engage in deals to profit from their name, image, and likeness ("NIL") without losing their amateur status and eligibility to compete in intercollegiate sports.¹⁰⁴ Student-athletes may now have the ability to negotiate individual commercial deals related to their ABD without losing eligibility. However, updated NIL regulation has not eliminated the power imbalance between student-athletes and their institutions; therefore, additional questions are raised as to whether schools may prevent student-athletes from individually profiting from their personal data by requiring athletes to sign over ownership rights in any ABD collected during their participation in the schools' athletics programs.

Finally, NCAA bylaw 15.3 provides terms and conditions for awarding, reducing, and cancelling student-athlete scholarships.¹⁰⁵ Essentially, scholarships cannot be reduced or cancelled for athletics-related reasons, such as injury, individual performance, or team performance.¹⁰⁶ Scholarships can, however, be reduced or cancelled if student-athletes engage in serious misconduct or do not meet non-athletic-related conditions of their scholarships, such as compliance with athletics department policies.¹⁰⁷ As such, student-athletes with multi-year

¹⁰¹ Note that student-athletes can and do benefit from ABD programs, as their personal performance and abilities are increased. This consideration alleviates some concern of exploitation, as the athletes do see benefit and are not simply exploited for no return. However, when considering the circumstances, exploitation is still evident, as the athletes likely have little choice in whether or not to allow their data to be used for the benefit of the entirety of their athletics program.

¹⁰² See Jessop & Baker, *supra* note 14, at 91-94.

¹⁰³ See, e.g., Arnold & Sade, *supra* note 3, at 69.

¹⁰⁴ Michelle Brutlag Hosick, *NCAA adopts interim name, image and likeness policy*, NCAA (June 30, 2021), <https://www.ncaa.org/about/resources/media-center/news/ncaa-adopts-interim-name-image-and-likeness-policy> [<https://perma.cc/HKF7-WXD2>].

¹⁰⁵ NAT'L COLLEGIATE ATHLETIC ASS'N, *supra* note 64, at 215-29.

¹⁰⁶ *Id.*

¹⁰⁷ *Id.*



scholarship agreements are safeguarded from having scholarships reduced or cancelled due to health or performance-related issues realized via ABD collection. In contrast, these provisions do not fully protect student-athletes from the intrusive, surveillance-based control discussed in Part II of this article, as institutions could potentially use ABD to allege behavioral misconduct or policy noncompliance as justification for scholarship cancellation. Further, student-athletes who are not on scholarship, or who are on single-year scholarships, are not protected from dismissal or non-renewal based on ABD.¹⁰⁸ Thus, NCAA regulation provides some, but not complete, protection from ABD being used to lower or eliminate a student-athlete's scholarship.

Family Educational Rights and Privacy Act ("FERPA")

Institutions of higher education are familiar with protecting student records, as FERPA prohibits disclosure of "educational records" without student consent.¹⁰⁹ Because FERPA broadly defines "educational records" as any materials that directly relate to a student and are maintained by the school, records beyond the classroom, such as those related to athletics participation, can fall within the statute's regulation.¹¹⁰ Thus, FERPA provides some promise as a means for regulating disclosure of ABD of student-athletes; however, the statute lacks sufficiency for addressing most concerns related to collegiate ABD collection.

To whom and to what does FERPA apply?

FERPA applies to any educational agency or institution, public or private, that receives federal funding from the U.S. Department of Education or whose students receive such funds and pay them to the institution—a designation most colleges fulfill.¹¹¹ FERPA defines "educational records" as "those records, files, documents, and other materials which (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution."¹¹² The statute provides that "directory information," such as name, email address, major, etc., do not

¹⁰⁸ Jessop & Baker, *supra* note 14, at 97-98.

¹⁰⁹ Matt R. Huml & Anita M. Moorman, *Student-Athlete Educational Records? The Involvement of FERPA Within Recent NCAA Division I Academic Scandals*, 27 J. OF LEGAL ASPECTS OF SPORT 127, 129-130 (2017).

¹¹⁰ *See id.* at 130-132.

¹¹¹ *FERPA General Guidelines for Students*, U.S. DEPARTMENT OF EDUCATION, <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/students.html> [<https://perma.cc/P3J2-5GGR>] (last visited Nov. 29, 2020).

¹¹² 20 U.S.C. § 1232g(a)(4)(A).



constitute educational records, and heights and weights of athletes as well as the officially recognized sports in which athletes participate are specifically noted as “directory information.”¹¹³ This specification suggests that other student records related to sport participation are, in fact, “educational records” under FERPA. ABD is information related to student-athletes and their participation in activities sanctioned by their schools, and it is retained by schools (or by ABD service providers acting for the institutions). Thus, ABD arguably constitutes “educational records” under FERPA’s regulation. However, because FERPA only applies to records that contain “information directly related to a student,” records or data points that are de-identified would fall out of the statute’s regulation.¹¹⁴ Therefore, while ABD that directly links to specific players may come within FERPA’s regulation, where ABD of a team is aggregated and de-identified, the records would not be “educational records” subject to FERPA protection. As previously discussed, de-identified student-athlete data has a reasonable likelihood of being re-identified (or linked back to the individual student-athletes). A high likelihood of “linkability” could keep de-identified ABD under FERPA’s governance.¹¹⁵ This discussion demonstrates that determining whether or not records fall under FERPA regulation is not a clear-cut undertaking. Nonetheless, without clear direction that ABD is not “educational records,” ABD arguably should be treated as falling within FERPA’s scope.

What protection does FERPA provide?

The stated purpose of FERPA is to “set out requirements for the protection of privacy of ... students.”¹¹⁶ The statute purports to protect privacy by prohibiting disclosure of educational records without consent of the student who is the subject of the records.¹¹⁷ Therefore, where records meet the requirements discussed above, FERPA requires that consent be received from the applicable student before the records be disclosed to third parties.¹¹⁸ Where institutions thwart this restriction, by engaging in a “policy or practice” of releasing records without authorization,¹¹⁹ FERPA authorizes the Secretary of the U.S. Department of Education to suspend the institution’s eligibility to receive funding from the

¹¹³ 20 U.S.C. § 1232g(a)(5)(A).

¹¹⁴ 20 U.S.C. § 1232g(a)(4)(A).

¹¹⁵ See Huml & Moorman, *supra* note 109, at 129-30.

¹¹⁶ 34 C.F.R. § 99.2.

¹¹⁷ 20 U.S.C. § 1232g(b) & (d).

¹¹⁸ *Id.*

¹¹⁹ 20 U.S.C. § 1232(g)(b)(1); See also *Gonzaga Univ. v. Doe*, 536 U.S. 273, 279 (2002).



Department.¹²⁰ Accordingly, FERPA may protect ABD from being disclosed by their schools to outside entities without student-athlete consent. However, as the following discussion demonstrates, FERPA's provisions fall short of affording solid protections for student-athletes.

First, in the 40 years of FERPA existence, no school has ever been penalized for FERPA violations with loss of its Department of Education funding eligibility.¹²¹ This lack of penalization does not mean schools have followed FERPA regulation without fail. Rather, widespread lack of understanding of FERPA's regulations and improper disclosures demonstrate that institutions are far from perfect in their compliance.¹²² Thus, to trigger penalties, FERPA violations must have to reach egregious and systemic levels, which has led to arguments that FERPA's enforcement measures are essentially ineffective.¹²³

Specifically in the sport context, a recurring theme of "sacrifice the athlete; protect the institution" partially characterizes institutions' relationship with FERPA.¹²⁴ In short, institutions have a reputation of overusing FERPA as a shield to avoid disclosures that could cast the institution in a negative light, while also violating FERPA by releasing information that does not cast the institution in a negative light, with little regard for the related student-athlete's privacy.¹²⁵ For example, evidence demonstrates institutions often release student-athlete academic honors and grade point averages to laud their academic achievement¹²⁶ and sometimes disclose negative academic records of student-athletes whose behavior has been unfavorable to the athletics program.¹²⁷ In contrast, institutions often refuse to release information that implicate them in academic scandals, NCAA

¹²⁰ Such a suspension would also disallow the institution from enabling its students to receive federal financial aid. 34 C.F.R. § 99.67.

¹²¹ Huml & Moorman, *supra* note 109, at 129.

¹²² Daniel J. Solove & Paul M. Schwartz, *INFORMATION PRIVACY LAW 1011-12* (Wolters Kluwer, 6th ed. 2017) (discussing misunderstandings of FERPA's regulations resulting in many cases of over-sharing or under-sharing of information, including emergency situations where disclosure is warranted based on safety implications).

¹²³ *Id.* at 1013.

¹²⁴ Huml & Moorman, *supra* note 109, at 138.

¹²⁵ Huml & Moorman, *supra* note 109, at 138-39; Paul J. Batista, *Student Athletes and the Buckley Amendment: Right to Privacy Does Not Include the Right to Sue*, 14 MARQ. SPORTS L. REV. 319 (2004).

¹²⁶ Batista, *supra* note 125, at 331; Jill Riepenhoff & Todd Jones, *Colleges Use Obscure Law to Keep NCAA Troubles Secret*, LEDGER, June 6, 2009, PROQUEST 390210909.

¹²⁷ See *Axtell v. Univ. of Tex. at Austin*, 69 S.W.3d 261 (Tex. App. 2002) (student's academic records given to radio station after student had spoken out against the coach and was released from the team for "academic reasons").



violations, or other potentially negative situations, even when that information is likely not FERPA regulated.¹²⁸

While a single instance, or even a handful of instances, of releasing ABD to a third party without student-athlete consent likely would not trigger penalties under FERPA,¹²⁹ a programmatic practice of authorizing third-party access to ABD without student consent would potentially rise to the level of egregiousness previously mentioned.¹³⁰ Institutions' controversial relationship with FERPA, coupled with a history of never being penalized for violation, however, raises concerns that institutions may not exercise the significant level of care that should be given to ABD programs, as mistakes are unlikely to result in penalty.

Second, in addition to having a penalty that has never been enforced, FERPA does not offer a means for individual redress, as the statute does not authorize a private right of action or create enforceable rights under 42 U.S.C. § 1983.¹³¹ Therefore, where ABD is disclosed without the consent of the student-athlete, the student-athlete has no remedy to seek. The student-athlete can instigate investigation of the institution by filing a complaint with the Family Policy Compliance Office; however, investigation can only lead to institutional implications and cannot bring individual redress to the student.¹³²

Third, FERPA only applies to records that directly link to a student, so the statute does not apply where data is de-identified.¹³³ Under this rule, intercollegiate athletics programs can authorize disclosure of aggregated, de-identified team ABD to third parties without FERPA implication. Self-regulation by colleges would, then, be the only means to ensure all data remained de-identified and student privacy remained intact, which is problematic for several reasons.¹³⁴ Teams may not be motivated to put significant resources toward monitoring ABD disclosure to ensure data remains sufficiently de-identified, given that likelihood

¹²⁸ See Huml & Moorman, *supra* note 109, at 133-36 (discussing the University of North Carolina's use of FERPA as a blanket defense for its refusal to release information related to an academic scandal, despite clear legal precedent of certain records not being FERPA regulated); Riepenhoff & Jones, *supra* note 126 (discussing many instances of institutions refusing to release information that likely was not FERPA regulated, such as Clemson University's refusal to release a photo of a high school athlete talking with a football coach in violation of NCAA recruiting rules).

¹²⁹ *Gonzaga*, 536 U.S. at 288.

¹³⁰ Solove & Schwartz, *supra* note 122, at 1013.

¹³¹ *Gonzaga*, 536 U.S. at 276.

¹³² Huml & Moorman, *supra* note 109, at 129.

¹³³ *See id.* at 129-30.

¹³⁴ *See* Osborne & Cunningham, *supra* note 4, at 47.



of punishment for inadvertent non-compliance is low.¹³⁵ Individuals in charge of the data programs may not fully understand the nuances of ABD and risks related to disclosure of identifiable data, which could lead to negligent authorizations of identifiable data.¹³⁶ Finally, due to the highly individualized nature of ABD, even with de-identification measures, insights provided by certain data points may still lead to re-identification of student-athletes.¹³⁷ Thus, while the data itself was not linked to an individual student when disclosed, the student-athlete's privacy would, nonetheless, be significantly implicated if third parties could analyze the data, use context and insights to identify the athlete, and glean knowledge of the athlete's personal characteristics.

Fourth, FERPA's disclosure regulation is premised on consent. Where an institution gains consent for disclosure from a student-athlete, the institution can share the student-athlete's information freely; however, FERPA does not set strict standards related to consent. The statute requires that consent be in writing, but it does not otherwise provide regulation as to what constitutes valid consent.¹³⁸ Thus, the consent requirement under FERPA does not alleviate concerns related to whether student-athletes are given a meaningful opportunity to refuse consent. Further, the statute requires that the written consent specifies the records that may be disclosed, the purpose of the disclosure, and the party or class of parties that may receive the information, but it does not require any further particularization or notice.¹³⁹ A blanket consent to ABD being disclosed to certain categories of third parties for the purpose of obtaining services and other consideration may be sufficient to allow an institution to disclose ABD that is protected under FERPA. Therefore, the FERPA consent requirements do not attenuate concerns that student-athletes may be truly informed about what they are authorizing and risking by providing consent to ABD disclosure.

¹³⁵ As a general rule, athletics programs and employees likely take protection of student-athletes seriously. Nonetheless, when the threat of punishment for noncompliance is extremely low, other issues easily become priority, resulting in less attention and resources being put toward those that are less likely to result in negative outcomes for the program.

¹³⁶ See generally *id.* (acknowledging that handling unprecedented amounts of data is a tall order for teams).

¹³⁷ *Id.* at 83.

¹³⁸ 34 C.F.R. § 99.30.

¹³⁹ *Id.*



Comparison of FERPA and HIPAA

The privacy and protection of health records is federally regulated by the Health Insurance Portability and Accountability Act (“HIPAA”), with the statute providing restrictions on how personal health information is used and disclosed by certain entities.¹⁴⁰ Because ABD is information intrinsically related to the health of the athletes, HIPAA is a reasonable framework to examine when considering ABD collection. However, based on how and by whom ABD is collected, applicability of HIPAA appears unlikely in most situations.¹⁴¹ Nonetheless, HIPAA’s protections are more robust than those provided by FERPA, so the statute is worth briefly examining in contrast with FERPA.

Where HIPAA does apply, entities are required to establish a privacy program and employ a privacy officer, train personnel on policies and procedures, and follow data security requirements.¹⁴² In addition to requiring consent for records to be disclosed, HIPAA sets specific rules around consent, including what constitutes acceptable authorization.¹⁴³ For example, specific authorization must be obtained for records to be used or sold for marketing purposes and, generally, authorizations are only valid if they detail the scope of the data use and disclosure in a “specific and meaningful fashion.”¹⁴⁴ Provision of treatment or benefits may not be conditioned on an individual’s consent to the information being disclosed.¹⁴⁵ The statute further aims to protect individuals’ privacy through the minimum necessary standard, which requires covered entities to take measures to only collect and use data actually needed to satisfy the particularized purpose of the data collection.¹⁴⁶ Finally, while HIPAA applies to certain “covered entities,” the statute also compels the business associates of covered entities, such as contracted data service providers, to comply with HIPAA’s privacy and security standards with respect to personal health information.¹⁴⁷

¹⁴⁰ Karkazis & Fishman, *supra* note 5, at 52.

¹⁴¹ See Smolenski, *supra* note 39, at 289-294 (providing a thorough discussion of HIPAA application to ABD in intercollegiate athletics, specifically noting that colleges and teams are likely not “covered entities” subject to HIPAA and that the U.S. Department of Health and Human Services has stated that new and emerging health technologies, like ABD collection devices, are not covered by HIPAA); Osborne & Cunningham, *supra* note 4, at 46-57 (providing a thorough discussion of HIPAA application to ABD in professional sports); Karkazis & Fishman, *supra* note 5, at 52-53 (providing an overview of HIPAA application to ABD in professional sports).

¹⁴² Solove & Schwartz, *supra* note 122, at 1013.

¹⁴³ 45 C.F.R. § 164.508.

¹⁴⁴ *Id.*

¹⁴⁵ *Id.*

¹⁴⁶ 45 C.F.R. § 164.502(b).

¹⁴⁷ 45 C.F.R. § 164.500.



FERPA does not set forth any of these standards or requirements, nor does it apply to business associates of educational entities that handle student records.¹⁴⁸ Instead, institutions dictate their own protective measures and authorization practices, undoubtedly resulting in varying standards across institutions and varying degrees of protection to emerging data types, such as ABD. Without compelled data security and privacy program minimums, banks of student ABD on university servers may remain vulnerable to hacking and breaches. Further, when schools contract with providers of devices, computing services, or cloud storage services, schools do not have set privacy and security standards they must require the contractors meet. Service provider contracts, thus, may not provide adequate protections to ensure the contractors do not misuse, improperly disclose, or insecurely store ABD.

As this discussion demonstrates, FERPA may provide some regulation for ABD disclosure, but it does not address many other concerns raised by ABD collection. Statutorily, FERPA does not provide robust protections, while the arguably ineffectual enforcement measures and inconsistent application of the statute raise concerns about motivations to zealously comply with its requirements.

Federal Trade Commission Act

In the United States' sectoral approach to data protection, the Federal Trade Commission ("FTC") holds some authority to regulate data practices for consumer protection.¹⁴⁹ While the FTC does not set standards for data protection, Section 5 of the FTC Act authorizes the FTC to protect consumers from unfair or deceptive practices in commerce.¹⁵⁰ In the context of data privacy and security, Section 5 is used by the FTC to ensure that companies uphold the data protection standards they claim to practice in their published privacy policies.¹⁵¹ Where companies do not follow their own privacy policies, the FTC may bring action against them for engaging in unfair or deceptive practices.¹⁵² Thus, if a company's policies state that it will not disclose data without permission, will only collect certain data, or will only use data for certain purposes, but the company is found to sell data

¹⁴⁸ See 20 U.S.C.A. § 1232g.

¹⁴⁹ See *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FEDERAL TRADE COMMISSION, <https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority> [<https://perma.cc/AL72-YBPF>] (last updated Oct. 2019) [hereinafter FTC Overview].

¹⁵⁰ *Id.*

¹⁵¹ See Solove & Schwartz, *supra* note 122, at 845-47.

¹⁵² See *id.*



to others or to collect or use data outside the scope stated in its policies, the FTC may seek action.¹⁵³

The FTC Act, thus, can regulate providers of ABD devices and services to some degree. Where institutions engage, as consumers, with providers whose policies claim certain data and consumer protection standards, the FTC is authorized to bring action where those standards are not being upheld.¹⁵⁴ For example, an ABD service provider's policies may assert that it does not use any data collected by or about its consumers for purposes of developing its own products. If the provider does, in fact, use ABD to develop and enhance its products, the FTC can bring an action against the service provider. However, as mentioned, this protection only extends to the prohibition of deceptive or unfair practices, such as divergence from posted company policies, and does not compel companies to publish certain data protection standards or to contract with consumers based on certain protective standards.¹⁵⁵ Therefore, the onus remains on institutions to only engage with companies that have strong data protection policies. Where institutions engage with ABD service providers whose posted data protection standards are lax or where institutions enter contracts with providers that do not adequately address data protection, the FTC has no enforcement authority to offer protections for the interests of student-athletes or their institutions.

California Privacy Rights Act ("CPRA") and Other Statutory Provisions

The CPRA, approved in late 2020, amended the California Consumer Privacy Act ("CCPA"),¹⁵⁶ the first comprehensive data privacy law enacted in the United States.¹⁵⁷ While the CCPA, and its subsequent replacement, specifically provide regulation for biometric data of California residents and data collected by certain California entities,¹⁵⁸ the effects and enforcement of this comprehensive, state-based approach to personal data regulation, as well as whether other states or the federal government will adopt similar frameworks, remain to be seen. Such statutes could provide significant personal data protections by establishing ownership rights in biometric data, setting forth strict standards for consent to sell or disclose data,

¹⁵³ See, e.g., *Sears Holdings Mgmt. Corp.*, 148 F.T.C. 83 (2009); *Snapchat, Inc.*, 158 F.T.C. 1095 (2014).

¹⁵⁴ See Solove & Schwartz, *supra* note 122, at 845-47.

¹⁵⁵ See FTC Overview, *supra* note 149.

¹⁵⁶ 2020 Cal. Legis. Serv. Prop. 24 (West).

¹⁵⁷ Protecting Personal Data: California Enacts First Comprehensive U.S. Privacy Law, The One Brief, <https://theonebrief.com/protecting-personal-data-california-enacts-first-comprehensive-u-s-privacy-law/> [<https://perma.cc/ZQF6-GPNH>] (last visited Nov. 29, 2020).

¹⁵⁸ Cal. Civ. Code § 1798.100 (West 2020); 2020 Cal. Legis. Serv. Prop. 24 (West).



creating limitations for the scope of data collection, and requiring widespread compliance of colleges, providers of wearables, and other third-party data seekers. Unless a similar omnibus regulation is enacted at the federal level, however, a litany of individual state regulations may not lead to uniform protections for the concerns raised by ABD collection in intercollegiate athletics.

Common Law Principles

Various common law principles may provide some basis for protection of student-athlete interests in ABD collection. First, the relationship between student-athletes and their institutions may create a duty of care specifically pertaining to consent and assumption of risk related to ABD. Though institutions do not possess in *loco parentis* responsibility creating a duty of care owed to the general student body, institutions have a special relationship with student-athletes, necessitating an increased standard of care related to their protection and development.¹⁵⁹ The recruitment process and coaches' pledges to develop athletes and guard their health, along with other factors, distinguish the relationship institutions have with student-athletes from that of the general student body, and student-athletes generally place much greater trust in their coaches and institutions than non-athlete students place in their institutions.¹⁶⁰ Consequently, institutions likely owe a greater responsibility to student-athletes, versus non-athletes, to ensure they understand the risks they assume when providing consent to the collection and dissemination of personal data.

Second, as no statutory frameworks discussed herein provide private rights of action for student-athletes to seek redress where ABD is improperly accessed, disclosed, or used, common law torts currently appear to be the main potential source of individual remedy. A full discussion of potentially applicable tort claims is beyond the scope of this article; however, causes of action could include public disclosure of private facts, where private information is shared against the subject's will; intrusion upon seclusion, where information about the subject is gained via intrusive means, whether information is shared publicly or not; appropriation of name or image, where the subject's likeness is used for others' gain; and false light, where publicity is given to inaccurate information about the subject.¹⁶¹ A prevailing tenet in U.S. law related to claims of privacy invasion or public disclosure, however, is the idea that once information has been willingly shared with others, the subject's privacy interest in that information

¹⁵⁹ Jessop & Baker, *supra* note 14, at 105-06.

¹⁶⁰ *Id.*

¹⁶¹ See generally Solove & Schwartz, *supra* note 122, at 81-232 (providing an overview of the various torts).



is nullified.¹⁶² Accordingly, student-athletes may be found to have little or no reasonable expectation of privacy in ABD they have willingly shared with their institutions or third-party ABD service providers,¹⁶³ making these potential remedies negligible.

Part IV: Suggestions for the Future of ABD

As discussed in Part III, no current frameworks provide robust protections for the concerns raised by ABD collection in intercollegiate athletics. Under current regulations, the collection and dissemination of ABD is permissible as long as consent from student-athletes is obtained or ABD is de-identified before it is shared with third parties. However, no standards exist to ensure consent is meaningfully obtained, data is only used for performance optimization, or that ABD does not become a means of oppressive surveillance. Further, colleges and their business associates—the ABD device and service providers—are not held to standardized policies of privacy and security to ensure data storage is adequately secure, data is not used or accessed improperly, and data remains properly de-identified. Instead, institutions, providers of ABD services, and third parties with interests in collegiate ABD are largely left to contract based on terms and standards they choose for the regulation of their own relationships, with the student-athlete being absent from the negotiating table and the contractual relationships. The following will outline ideals to strive for in ABD regulations and programs in intercollegiate athletics and will provide specific considerations for various entities and regulatory frameworks.

Fair Information Practice Principles

In response to the growth of data processing and growing concerns about privacy and rights in personal data collected and stored by various agencies, the Department of Housing, Education, and Welfare issued a highly influential report on data privacy in which it recommended a Code of Fair Information Practices (“FIPs”).¹⁶⁴ While the FIPs do not provide statutory regulations for data processing, they provide a framework of rights and responsibilities for those whose data is collected and those who do collecting, respectively.¹⁶⁵ The FIPs have significantly influenced the framing of privacy regulations globally,

¹⁶² See, e.g., *id.*

¹⁶³ See, e.g., *Dwyer v. Am. Express Co.*, 652 N.E. 1351 (Ill. App. Ct. 1995) (consumers voluntarily shared information with credit card company and, thus, lost right to privacy and ability to seek tort remedy when certain information was shared with other entities).

¹⁶⁴ Solove & Schwartz, *supra* note 122, at 663-64.

¹⁶⁵ *Id.*



with the Organization for Economic Cooperation and Development's ("OECD") articulation of the FIPs being the most well-known.¹⁶⁶ The OECD's articulation is as follows:

- (1) Collection Limitation—Collection of personal data should be limited and data should only be obtained through lawful, fair, and consensual practices.¹⁶⁷
- (2) Data Quality—Personal data collected should be relevant to the purposes of their use and should be kept accurate and updated.
- (3) Purpose Specification—The purposes of the collection should be stated prior to collection and use should be limited only to those purposes.
- (4) Use Limitation—Personal data should only be disclosed or made available for use other than the stated purposes with consent of the subject or by authority of law.
- (5) Security Safeguards—Reasonable security safeguards should be in place to protect personal data against unauthorized access, use, disclosure, or modification.
- (6) Openness—A general policy of openness about the practices and policies of data collection, the data that exists, and the identity and status of the data controller.
- (7) Individual Participation—Data subjects should have the right to obtain data related to her in a reasonable timeframe and to challenge the accuracy of said data.
- (8) Accountability—Data controllers should be accountable for complying with personal data protection measures.¹⁶⁸

The FIPs stress that personal data should only be used for the specific purposes for which it is collected, collection and use of data should be completed with transparency, collection should be minimized such that only data necessary for stated purposes is collected, security of data should be prioritized, and the controller of data should be accountable to the data subject for data protections.¹⁶⁹ While these principles are not statutory requirements, they provide a set of ideals by which entities collecting, using, or storing data should abide.¹⁷⁰

¹⁶⁶ *Id.*

¹⁶⁷ ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, THE OECD PRIVACY FRAMEWORK 14-15 (2013).

¹⁶⁸ *Id.*

¹⁶⁹ *See id.*

¹⁷⁰ *See id.* at 13-14.



Considerations for NCAA Regulation

While the NCAA has no obligation to student-athletes, as its relationship is with institutions, not athletes, the NCAA would nonetheless be well served by proactively regulating ABD collection practices of its member institutions.¹⁷¹ Upholding its commitment to ensuring student-athletes are students first and are not unreasonably exploited is reason enough to regulate ABD practices, while building goodwill with student-athletes and other interested parties by creating regulations that ensure student-athlete interests are upheld is further reason.

Because the NCAA is not a state actor,¹⁷² it is not limited by constitutional doctrine and can regulate practices without liability for being restrictive of speech or other rights. Thus, the NCAA may be able to impose restrictions on how and what data is collected, how it is used, and when and if it can be disclosed or sold to third parties, more freely than federal regulation could.¹⁷³ Though, antitrust concerns could arise should the NCAA attempt to place caps on ABD pricing or require data to only be licensed to certain entities.¹⁷⁴

In seeking to regulate ABD collection, the NCAA should use the FIPs as foundational principles to outline rights and protections for student-athletes balanced against interests and responsibilities of institutions. Limitations on the scope of ABD collection and use—on what can be collected and how it can be used—could protect student-athletes from unreasonable intrusions and control exerted by coaches. Security requirements, such as how data may be transferred and stored and limitations on who may access or control data within institutions, would help protect against certain abuses and ensure data remain secure, only accessible by appropriate parties, and de-identified, as necessary. Strict requirements for transparency and obtaining meaningful consent would help to ensure student-athletes are not pressured into providing consent, are aware of what ABD collection will entail and who may access their data, and are informed of the risks related to ABD collection, use, and disclosure. Blanket consent for all programmatic collection and dissemination of ABD is not sufficient. Instead, consent should be required on a more particularized basis, per collection method, purpose, third-party relationship, etc. Specific guidance should also be provided as to how ABD programs might implicate bylaw 2.9's protection against commercial exploitation of student-athletes and how institutions can engage in ABD programs without unreasonably exploiting athletes.

¹⁷¹ Jessop & Baker, *supra* note 14, at 111.

¹⁷² *Nat'l Collegiate Athletic Ass'n v. Tarkanian*, 488 U.S. 179 (1988).

¹⁷³ See *infra* notes 176-78 and related text.

¹⁷⁴ See, e.g., *Nat'l Collegiate Athletic Ass'n v. Bd. of Regents of Univ. of Okla.*, 468 U.S. 85 (1984).



The NCAA might also consider providing best practices guidelines, training, and contract provision templates for athletics departments seeking to engage in ABD collection. In addition to training for institutional personnel, providing training for student-athletes would contribute to their understanding of the implications of ABD collection and ability to meaningfully provide or deny consent. Finally, the NCAA could form a committee or other body to vet ABD services and practices before they are used by athletics departments, similar to the committee formed by the NFL CBA previously discussed.¹⁷⁵ This practice would enable the NCAA to provide guidance as to which services and practices adequately serve the interests of both institutions and student-athletes and to establish minimum standards by which all service providers must abide.

Considerations for FERPA Modification

Modification of FERPA to more closely align with the regulations provided by HIPAA would address some of the concerns discussed herein. First, the addition of privacy and security standards to FERPA would streamline data protections across institutions and would hold athletics departments' ABD collection to those standards. These standards should include, among other things, security requirements for data storage and transmission, limitations on data access, and protocols for de-identification of data. Second, business associates that provide data-related services to educational institutions should be held equally responsible for following these FERPA standards. If FERPA applied to business associates, data protections would not depend on individual contracts between institutions and ABD service providers or on the providers' own policies but would, instead, be federally standardized. Third, FERPA training specific to technical and nuanced information, such as ABD, should be required for all who handle educational records to decrease chances for data to be improperly used or disclosed, and to encourage opportunities for meaningful consent to be provided where data is disclosed to third parties. Fourth, FERPA should have more meaningful enforcement to ensure institutions are motivated to follow its regulations. Finally, FERPA's consent standards should be heightened to ensure students' consent is both informed and meaningful.

In revisiting FERPA regulations, specific consideration should be given to both the idea of institutions selling student data for financial gain and institutions engaging in surveillance-like data collection. These are both practices that likely were not at the forefront of consideration when FERPA was established, but

¹⁷⁵ Because the NCAA regulates intercollegiate sport at different levels of competition (Division I, II, and III), all three divisional levels would need representation in the vetting process to ensure approved practices and services are accessible by and representative of the needs of institutions and student-athletes at all levels.



with these practices increasing, specifically in the athletics context, regulation to prevent the exploitation and unreasonable control of students could come by way of FERPA regulations. For example, the following considerations would provide additional protection of student-athletes' interests pertaining to ABD: (1) more robust and particularized requirements for obtaining consent for disclosure, especially where that disclosure is for monetary gain of the institution; (2) data minimization requirements that compel institutions only to collect data necessary for stated purposes, such as enhancing students' educational experience, to minimize collection of exorbitant amounts and unnecessary types of data; (3) limitations on institutions attempting to collect and store data related to personal devices of students or devices worn by students outside of official institutional activities.

A potential limitation on FERPA's ability to protect student interests, specifically where the sale of data is involved, is First Amendment commercial speech doctrine. FERPA may be unable to restrict institutions from selling student data for specific uses deemed most likely to exploit students, such as for sports content production, as such restriction could be deemed an unconstitutional content-based restriction on commercial expression.¹⁷⁶ In *Sorrell v. IMS Health*, for example, the Supreme Court addressed a state law that prohibited the sale of pharmaceutical prescriber-identifiable data for purposes of marketing certain prescription drugs.¹⁷⁷ The Court held the restriction was an unconstitutional restriction of speech because it burdened certain expression, based on the content of the speech, rather than being a content-neutral restriction.¹⁷⁸ Thus, should federal law seek to regulate use and disclosure of ABD, it must do so without unconstitutionally restricting expression via content-specific regulations, as seen in *Sorrell*.

Considerations for Colleges

Colleges have multiple interests in ABD, including performance enhancement and financial gain, but in developing ABD collection practices, institutions must also bear in mind the sometimes-countervailing interests of student-athletes, as well as the prying interests of third parties. When institutions enter relationships with ABD device or service providers, student-athlete data is automatically shared with a third party—the service provider. Thus, whether institutions are negotiating contracts to obtain ABD services or to license ABD to other parties, institutions should require that contract provisions follow the FIPs to ensure privacy rights are upheld, data is only used and disclosed for the limited purposes

¹⁷⁶ See, e.g., *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011).

¹⁷⁷ *Id.* at 557.

¹⁷⁸ *Id.* at 580.



set forth in the agreement, and the parties are accountable for the security and privacy of the data.

In addition to the relationships institutions enter with third parties, they must also be intentional in their relationships with student-athletes. Because of the special relationship that exists between student-athletes and their institutions, athletics programs should ensure student-athletes are informed of their rights and risks as they pertain to ABD collection, use, and disclosure and have meaningful opportunities to deny consent for participation in ABD programs. Further, institutions should ensure coaches and other personnel who engage with ABD have adequate training on how to effectively and appropriately use the data, on restrictions related to use and disclosure, and on risks of inappropriate use and disclosure, to avoid the concerns discussed herein.

Conclusion

While far more questions about ABD collection in intercollegiate athletics have been raised than answered in this paper, they are questions worth probing and answers worth demanding, as they implicate young athletes and a rapidly developing industry. The surface has only been scratched in ABD collection. Biometric data can substantially positively impact sport by facilitating research, promoting safe training practices, increasing the efficacy of rehabilitation methods, and more. However, those benefits come with risks of privacy invasion, exploitation, and abuse. As such, regulations to protect student-athletes' interests must be established and questions surrounding use, ownership, control, and security of data must be addressed before negative implications are widely felt.

