Spring 4-12-2021

Biometric Performance Monitoring in Collegiate Sports: Balancing the Benefits with Ethical and Regulatory Considerations

Daniel Haugen
dlhaug7343@ung.edu

Biometric Performance Monitoring in Collegiate Sports:

Balancing the Benefits with Ethical and Regulatory Considerations

A Thesis Submitted to

The Faculty of the University of North Georgia

In Partial Fulfillment

Of the Requirements for the Degree

Bachelor of Science in Computer Science

With Honors

Daniel Haugen

Spring 2021

Abstract

Biometric performance data provides invaluable insights into an athlete's performance, which coaches can utilize to optimize training sessions and help prevent and track player injuries. This research contrasts the importance of biometric performance data in sports with the necessity for protecting that data as it is collected by wearable performance monitoring devices and then utilized within collegiate sports. Several ethical and security concerns are fostered by the lack of explicit regulations protecting student-athletes' biometric performance data. Therefore, an analysis is provided of the regulated protections provided to professional athletes and collegiate athletes for collecting, storing, and utilizing their performance data. Furthermore, this paper examines the implications of Murphy v. NCAA and its revocation of federal regulations prohibiting sports wagers on both professional and amateur athletics. Finally, this paper presents a set of potential reforms to regulations and legislation that could provide additional safeguards preventing the unauthorized disclosure of student-athlete biometric performance records.

Biometric Performance Monitoring in Collegiate Sports:

Balancing the Benefits with Ethical and Regulatory Considerations

Biometric data relates to any bodily measurement that can be utilized to uniquely identify individuals based on their human characteristics through physiological or behavioral traits (Osborne, 2017). These distinct measurements provide vital characteristics that, once combined with traditional athletics performance data (e.g., acceleration, velocity, distance), uncover endless possibilities for additional analysis and metrics for determining a player's workload, injury recovery status, and areas of their sport in which these athletes can improve.

Although biometric data is commonly thought of as the external characteristics that make every individual unique, biometric performance monitoring often integrates the internal characteristics that distinguish individuals. Khan et al. (2020) describe these classifications as extrinsic and intrinsic biometric characteristics. Specifically, extrinsic biometric traits related to an individual's external physical characteristics, including physical appearance or other physiological biometrics, such as someone's fingerprint. In contrast, intrinsic biometrics encompass internal biological characteristics such as blood pressure, heart rate, and further traits that could be linked to a particular identity (Khan et al., 2020). Both categories of biometric characteristics distinguish one individual from another and provide an outlet for verifying an individual's identity.

This research explores the protections that are in place to regulate the collection, storage, and utilization of biometric performance data gathered from student-athletes during training sessions and matches. As states continue to legalize sports betting on professional and collegiate athletics, the onus falls on federal, state, and league-specific regulations to ensure the protection of student data that may be a growing target for cyber intrusions. Under current regulations,

students' athletics records—which have traditional personally identifiable information removed to de-identify the dataset—may still risk re-identifying players due to the unique characteristics inherently involved with biometric records.

Importance of Performance Data in Sports

The abundance of additional sensors integrated into modern athletics trackers fosters innovation in biomechanical research for establishing novel proprietary algorithms that produce accurate and reliable performance metrics. For example, a case study of professional Australian football players allowed for the development an accelerometer-based energy metric that provides comparable accuracy and reliability to the manual review of the video analysis from the experiments (Wixted et al., 2007). Furthermore, as the findings suggest in a recent case study developed by Fox et al. (2021), monitoring the sleep patterns of athletes prior to competition dates may provide valuable insights into a correlation between athlete sleep patterns and athletic performance during matches.

Most notably, biometric performance data provides new mechanisms for objectively determining factors and metrics that used to be ascertained through subjective self-reporting of athletes, such as perceived exertion or recovery status from an injury. For instance, training load metrics provide athletics trainers additional insights into the capability of a player to return to regular training sessions and matches following an injury spell. These training load metrics can provide data for tracking a player's "local tissue capacity and sport-specific capacity," which provide vital metrics for a player's muscular state and ability to return to the stressful environment of regular matches (Gabbett, 2020). Similarly, sleep monitoring devices provide objective statistical evidence of sleep disruption—a common symptom of traumatic brain injury—and previously relied on self-reporting of player symptoms to help diagnose (Cummins,

2017). Therefore, players would no longer have the same leverage in falsifying the state of their condition now that there are additional forms of evidence to the contrary.

Ethical Considerations Regarding Biometric Performance Data

When operating with student-athlete performance data, certain levels of ethical and legal criteria must always be considered and preserved given the specificity and personalized nature of the data being collected, stored, and analyzed. Analysts, their performance monitoring devices, and the tools they utilize for systematically aggregating and analyzing the raw data must ensure the reliability and accuracy of the data being collected and presented. Failure to present an accurate representation of a player's physiological well-being and work rate may inadvertently or incorrectly damage a player's reputation and ability to retain athletic scholarships or potential professional contracts resulting from faulty algorithms or the misinterpretation of the generated analytics. Furthermore, the data collected and stored for these purposes must prioritize the security of the systems and databases storing these biometric data points to prevent data breaches and limit security risks.

Data Collection and Informed Player Consent

Athletic performance data collected by teams during training sessions and matches provide invaluable insights into their athletes' fitness, but coaches must ensure that their performance metrics are appropriately calculated and interpreted. Many sports tracker manufacturers and service providers integrate global positioning system (GPS) sensors into their devices to coordinate with heart rate monitors, accelerometers, and a plethora of other sensors to aggregate the collected raw data into proprietary algorithms for determining player performance (Li et al., 2016). Although most metrics are reasonable and relatively non-intrusive, some services may collect data that begins to infringe on the privacy of an individual. For instance,

WHOOP, a significant player in the athletic performance monitoring marketplace, tracks athletes' sleep patterns, alcohol consumption, and even requests input on levels of an athlete's sexual activity to produce a recovery metric for each athlete's calculated performance readiness level (Jessop & Baker, 2019). While the requested metrics have their purpose for the final calculation, some players and coaches might view this level of detail as more of a surveillance mechanism than a performance tool.

In contrast to the WHOOP sensors designed for all-day tracking, even throughout an athlete's off-field activities, most devices designed for collegiate athletics are meant for use during matches and training sessions (Balletta, 2020). Furthermore, these devices passively collect a player's performance data through sensors that are often strapped to a player's chest, wrist, or on their back in-between their shoulder blades, as found with devices from another major manufacturer, Catapult (Li et al., 2016). Similarly, innovative sensors like the devices developed by WiSP are worn as highly flexible bandage-like patches that contain sensors for tracking a vast array of biometric metrics, including unique metrics like brain activity, blood pressure, and chemicals present in players' sweat (Karkazis & Fishman, 2017).

Therefore, compared to traditional medical screenings, the data collection process in modern wearable trackers is relatively non-intrusive given the vast array of generated metrics coming from these devices. However, there is also little regulation to ensure the quality and accuracy of each performance analytic developed through a service's proprietary algorithms (Khan et al., 2020). Therefore, inaccurate metrics derived from a player's sleep patterns or subjectively reported external activity metric may theoretically influence a coach's decision-making for a match lineup or potential extension of a player's athletic scholarship (Casher, 2019).

Data Utilization and Ownership

As the commercialization of student-athletes' performance data continues to grow in stature, schools will have to establish additional safeguards to ensure that the biometric data being shared with external corporations and partners does not lead to a negative impact on their student-athletes (Studnicka, 2020). While corporate partnership deals like the over $170 million contract between the University of Michigan and Nike, in exchange for 15-years of access to the university's athletic performance data, illustrate the magnitude of importance that is placed on performance analytics in collegiate sports, it also raises concerns over who owns the datasets and what protections are in place to safeguard the records of these athletes.

Even though federal regulations have provided limited explicit clarification on the protections afforded to collegiate athletes on the commercialization of their identity, states like California are taking steps to ensure that players have a more significant influence on the monetization of their collegiate athletic career. On September 30th, 2019, Senate Bill 206—more commonly known as the Fair Pay to Play Act—permits student-athletes to acquire sponsorship deals and partnerships with corporations that do not conflict with the partnerships of their university (Studnicka, 2020). Although the Fair Pay to Play Act will not go into effect until January 1st, 2023, it has provided a precedent for other states to follow in its place and apply pressure on the NCAA to lessen its regulations on the amateurism of collegiate sports.

Although most of the benefits provided by the utilization of biometric performance data come from gaining additional insights into specific attributes of a player's performance, corporate partnerships and biomechanical research should only be provided de-identified performance data to ensure that the metrics are integrated ethically. While traditional identifiers like player name, number, and any other traditional personally identifiable information can easily

be removed from the dataset prior to sharing with external parties, the biometric and biomechanical data collected by these sensors are far more difficult to de-identify due to the intrinsically unique nature of some of these statistics such as a player's heart rate patterns. Therefore, it would still be feasible for an external party to utilize these statistics to link the performance metrics to their respective athletes (Osborne, 2017).

Data Storage and Security Preventatives

As wearable performance monitors become more advanced to include additional sensors and account for performance metrics, organizations must ensure that the aggregated datasets are appropriately protected to prevent data breaches and misuse of the generated analytics. Since most athletics trackers are low-power networked devices configured to transmit data real-time to coaches and cloud servers, additional confidentiality and integrity issues may arise from the loose security measures established in most Internet of Things (IoT) devices (Khan et al., 2020). Furthermore, large athletic tracking device distributors, such as Catapult, provide additional cloud services and have lucrative partnerships with teams across all of the prominent U.S. professional and collegiate sports teams. These service providers must ensure that their systems and databases are heavily secured as they essentially serve as a centralized repository of all their clients' athletic performance data, and a security breach of that magnitude may be detrimental to not only the reputation of the sport but to the individuals that are victimized by the breach.

One of the most renowned instances of data breaches in recent sports history involves the hacking scandal surrounding the invasion of the Houston Astros' internal proprietary scouting database by an employee of a competing organization, the St. Louis Cardinals. In early 2016, Chris Correa, the former scouting director of the Cardinals, plead guilty to hacking into the Astros' analytics database known as "Ground Control" on several occasions throughout 2013

and 2014. In violation of the Computer Fraud and Abuse Act (CFAA), Correa gained unauthorized access to the Astros' email accounts and servers containing scouting lists for draft players, trade-secrets, potential employee bonuses, and notes on player injuries and performances (Williams, 2019). Furthermore, Major League Baseball (MLB) commissioner Rob Manfred placed Correa on the MLB's "permanently ineligible list," prohibiting Correa from working in any capacity within the sport, before forcing the Cardinals to pay the Astros $2 million in restitution and hand over the first two picks of the 2017 MLB Draft (Grow & Shackleford, 2020).

Although the organizations involved in these controversies may receive some vindication from the resolution of criminal proceedings, these engagements may only serve as formalities compared to the potential damages caused by a data breach leaking players' biometric performance data (Osborne, 2017). The reactionary nature of sports leagues towards cybersecurity protections opens the leagues and their teams to reputational damage caused by lax cybersecurity regulations and poor cybersecurity hygiene (Henne, 2017). For example, Russian hacktivist group Fancy Bear successfully hacked into the World Anti-Doping Agency during the 2016 Summer Olympic Games, releasing forty-one athletes' confidential athletics data across thirteen different countries (Williams, 2019). Similarly, in early 2014, the Syrian Electronic Army (SEA) hacked into the official club Twitter account of FC Barcelona, one of the most recognized soccer clubs in the world, to spread their extremist messages while masqueraded as authorities within the organization (Williams, 2019).

Regulatory Protections

With the rapid growth in the integration of athletic performance data in the day-to-day operations of collegiate and professional sports, mandated regulations must be implemented to

ensure that every sports organization and institution remains compliant with a minimum standard of protection over the vast amounts of performance data gathered from their athletes. The differentiating protections provided to professional athletes in contrast to their collegiate counterparts, and vice versa, are explored in the following section. Furthermore, this section discusses the protections provided by the Family Education Rights and Privacy Act (FERPA) for collegiate athletes since they are not considered employees of their universities and are, therefore, not afforded the additional protections and capabilities provided to their professional colleagues.

Protections for Professional vs. Collegiate Athletes

Collegiate athletes are not provided the same level of protection that professional athletes are allocated when it comes to the legal bargaining power for protecting their performance data. As Barbara Osborne (2017) notes in her analysis of the laws and regulations surrounding professional athletes' athletic performance data, "no federal laws exist to specifically regulate biometric data collection". Osborne (2017) continues to note that biometric data is often not classified as "personal health information (PHI)," and as such, teams would not be mandated to regulate their utilization but would rather often self-regulate their procedures and protocols for protecting athlete data since it is not specifically enforced through HIPAA.

For professional players, the Department of Health and Human Services (DHHS)—responsible for overseeing HIPAA compliance—has claimed that even if HIPAA did apply to professional athletes' performance data, players' clubs would likely be capable of side-stepping HIPAA regulations by listing biometric performance data as employment records, removing it from the jurisdiction of HIPAA (Brown & Brison, 2020). Therefore, in recent years, the emphasis has been placed on the collective bargaining agreements (CBA) for the respective

professional leagues to ensure that professional athletes' voices and concerns are heard regarding the utilization and protection of their performance data. However, in contrast to the CBAs offered to professional athletes for negotiating the rights to their biometric performance data, NCAA athletes are absent from any such capability since collegiate athletes are not considered employees under federal legislation and are not unionized (Jessop & Baker, 2019).

Furthermore, under current NCAA regulations, collegiate athletes are prohibited from earning financial rewards for their work past the educational scholarships provided by their universities. These limitations are in stark contrast to their professional counterparts and demonstrate the inherent flaws with the current standing regulations. As the commercialization of athletic performance data continues its exponential growth, student-athletes remain left with few options for protecting their biometric data as it continues to be monetized for hundreds of millions of dollars by their university and its corporate partners (Lazan & Greenbaum, 2017). Under these restrictions, the power and ownership for the fate of the biometric performance data are controlled by the university athletic department to determine the outcome and utilization of the generated analytics (Henne, 2017).

Family Education Rights and Privacy Act (FERPA)

All schools that acquire federal funding through the U.S. Department of Education must remain in compliance with the regulations set forth in the Family Education Rights and Privacy Act (FERPA). First enacted in 1974, this federal legislation provides students greater control over the disclosure of personally identifiable information contained within their educational records. While most records protected by FERPA relate to a student's personal information and academic records, the 2008 amendments added additional forms of personally identifiable

information. Most notably, § 99.3 provides the following definition and examples of biometric records:

> Biometric record, as used in the definition of personally identifiable information, means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting. (34. C.F.R. § 99.3, 2008)

Under FERPA's guidelines, personally identifiable information (PII) refers to information within educational records that could be used to link any particular record or set of records to the identity of a student through both direct identifiers, including a student's name or student ID number, or indirect identifiers, like a student's birthdate or place of birth. Therefore, if all instances of PII are redacted from the dataset, institutions are permitted to release the information since all the data has been de-identified. However, issues may arise regarding the level of de-identification that should be required for a student-athlete's biometric performance records to be considered fully anonymized.

Although a student's athletic performance data is not explicitly listed within the regulation or its definition of biometric records, it is feasible—based on the level of sophistication and abundance of biometric metrics recorded in modern athletic tracking devices—for an individual with access to de-identified metrics to match a player to their respective performance records. Information, such as biometric records that could be utilized to link to any specific individual, would theoretically be far easier to attribute to a player within the team since the collection of student-athletes at a university would be far less populated than the

general student population. Therefore, careful considerations should be taken to handle the release of collegiate athletes' biometric performance data.

Implications of Sports Betting

In early 2018, the U.S. Supreme Court case Murphy v. National Collegiate Athletic Association (NCAA) found the Professional and Amateur Sports Protection Act of 1992 (PASPA) unconstitutional under the tenth amendment (Williams, 2019). This landmark decision removed federal regulations which had prevented sports betting in all states other than Nevada, therefore, allowing states to develop their own independent legislation for permitting or prohibiting online and in-person sports betting. The push for this decision was heavily advocated by both the sports leagues looking for additional ways to monetize the data they were already collecting and the states that were interested in further tax revenue gained from regulating the sports betting industry that was littered with illegal betting activity (Kaburakis, et al., 2015).

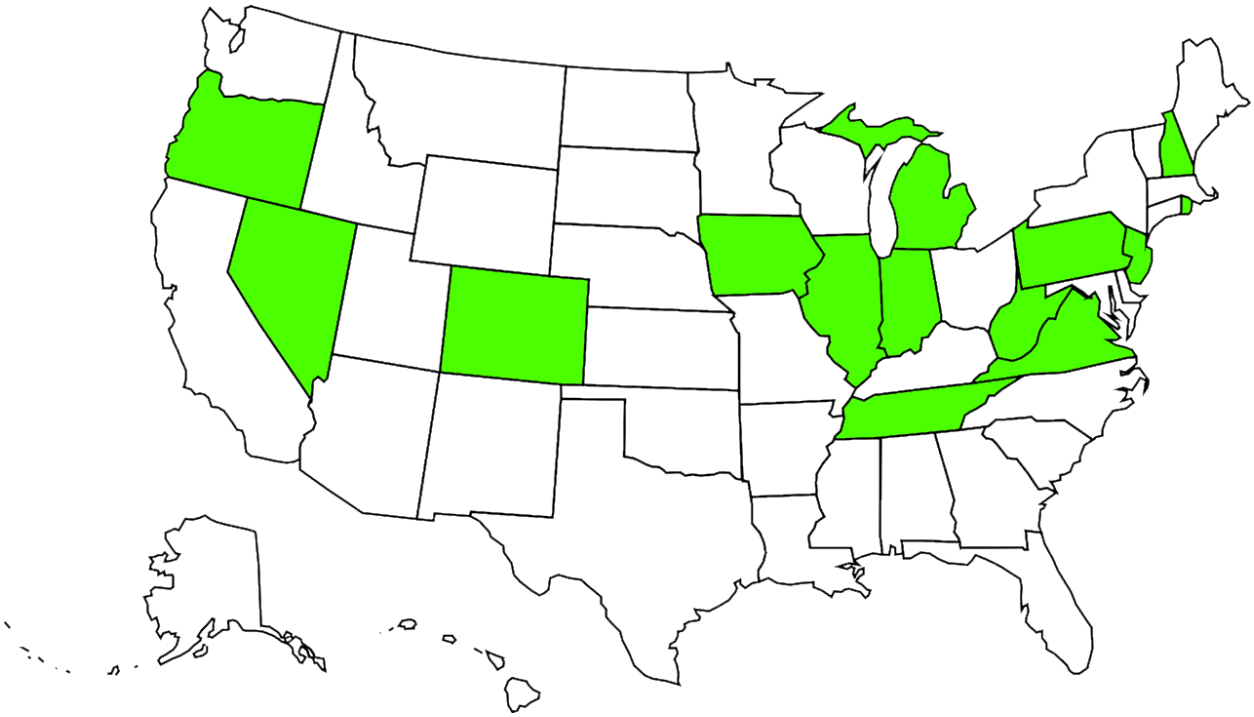
Sports leagues are monetizing performance data through sports betting in two primary methods. The first scenario involves leagues selling data directly to individuals or groups that are active in sports betting procedures (Rodenberg, 2021). Alternatively, the more prevalent option involves leagues working with external data brokers to distribute "official" statistics through potentially exclusive partnerships (Grow & Shackleford, 2020). The justification provided by many professional leagues for the commercialization of official datasets is to produce a league-approved recount of the events and performance of players within matches to validate the accuracy of the records (Williams, 2019). However, some states have enacted restrictions prohibiting individuals from placing wagers on in-state collegiate teams to deter student-athletes from potentially fixing matches based on the current wagers for a match. A potential resolution that would ensure collegiate athletes would not be inclined to make such decisions and

concurrently reduce the incentive of individuals to obtain unauthorized access to this data is to prohibit sports betting on collegiate athletics, as already is the case in several states.

To confirm that individuals comply with state mandates on the legalization of the state they are in, virtual borders around states have been constructed using geofencing to prohibit online sports betting in areas that have not enacted legislations permitting online betting (Fortunato, 2020). These restrictions rely on the GPS functionality built into smartphones to provide expansive coverage in states that permit online betting anywhere within the state. On the other hand, in certain states like Arkansas that only permit sports betting in licensed casinos, more accurate forms of geolocation are required, such as Bluetooth connectivity. However, these virtual borders are difficult to enforce as the utilization of a virtual private network (VPN) can spoof the GPS coordinates of a device to appear from anywhere else in the world. The map illustrated in Figure 1 below presents the fourteen states that have legalized online sports betting from anywhere within the state:

Figure 1

States That Have Legalized Online Sports Betting



Note. The 14 States, plus Washington DC, that have legalized online sports betting within the United States.

Proposed Reforms

Professional and collegiate sports must move away from their inclination to perform in a reactive posture toward modern cybersecurity concerns brought on by the integration of new innovations within the sport. A more forward-thinking, proactive approach to cybersecurity will further safeguard the private information maintained by athletic entities without retroactively responding to data breaches and other incidents that damage the reputation of the league and risk the confidentiality of player data (Grow & Shackleford, 2020). Additional reforms to either federal legislation, through HIPAA or FERPA, or amendments to league requirements should be implemented to ensure a minimum standard of security for the protection of athlete data during the process of collection, storage, and utilization.

Potential modifications to current federal legislation could include the expansion of FERPA to include specific protections provided by HIPAA for ensuring the confidentiality and integrity of student athletic records. For example, if HIPAA applied to collegiate athletes'

medical records, colleges would be required to hire a compliance officer to institute and enforce ancillary practices to further prevent the disclosure of athlete medical information (Smolenski, 2019). Alternatively, federal or state legislation should mandate that colleges remain in compliance with the security requirements outlined in HIPAA's Privacy and Security Rules. Notably, HIPAA's Security Rule would require institutions to ensure "physical, administrative (include risk analysis measures), and technical (including access and transmission) security safeguards are in place for protecting PHI" (Osborne, 2017).

Furthermore, as more states continue to legalize in-person and online sports betting, organizations such as the Sports Wagering Integrity Monitoring Association (SWIMA) must continue to prohibit suspicious behavior aimed at obtaining unfair advantages through compromising the integrity of betting procedures or illegally obtaining athletic performance data (Williams, 2019). With the revocation of the federal prohibition of sports betting and the inclination of states to legalize their own individual legislation, there should be some regulations to mandate a minimum level of protection shared across all state legislation.

Conclusion

Biometric performance data plays an invaluable role in the day-to-day operations of most professional and collegiate sports teams. However, regulations have not kept pace with the swift innovation and integration of proprietary performance metrics aimed at providing reliable and accurate insights into objective statistics that can be utilized by coaches. Particularly, collegiate athletes are provided even less power and leverage over the collection, storage, and utilization of their performance data compared to their professional counterparts. With the ruling of Murphy v. National Collegiate Athletic Association (NCAA), many states have legalized their own

independent sports betting regulations which may incentivize hackers to target player data to obtain unfair advantages for financial gain.

This research has explored the current landscape of rules and regulations applying to student-athlete performance data. Issues of ethical concerns and cybersecurity risks have not been adequately addressed by current regulations within the United States. Therefore, additional reforms should be implemented at either a federal, state, or league level to protect the performance data that could potentially be linked to a specific athlete, even with traditional forms of de-identification. Future work should explore the protections provided to collegiate athletes outside of the U.S. to contrast the regulations on the biometric performance data of student-athletes within different counties. Additionally, research should explore the extent of de-identification that would reasonably ensure the de-identification of biometric player data.

References

34. C.F.R. § 99.3 (2008).

Balletta, J. A. (2020). Measuring Baseball's Heartbeat: The Hidden Harms of Wearable Technology to Professional Ballplayers. Duke Law & Technology Review, 18, 268–292.

Brown, S. M., & Brison, N. T. (2020). Big Data, Big Problems: Analysis of Professional Sports Leagues' CBAs and Their Handling of Athlete Biometric Data. Journal of Legal Aspects of Sport, 30(1), 63–81.

Casher, C. (2019). Moneyball in the Era of Biometrics: Who Has Ownership over the Biometric Data of Professional Athletes? Dalhousie Journal of Legal Studies, 28(1), 1–28.

Cummins, P. (2017). TBI and NFL Culture: Can Players Autonomously Refuse Biometric Monitoring? American Journal of Bioethics, 17(1), 75–77. https://doi-org.proxygsu-nga1.galileo.usg.edu/10.1080/15265161.2016.1251645

Fortunato, J. A. (2020). Producing and Promoting the Sports Gambling Industry since the 2018 United States Supreme Court Ruling: A Review of Organizational Action through Suspense Theory. Journal of Gambling Business & Economics, 13(1), 117–133. https://doi.org/10.5750/jgbe.v13i1.1807

Fox, J. L., Stanton, R., Scanlan, A. T., Masaru Teramoto, & Sargent, C. (2021). The Association Between Sleep and In-Game Performance in Basketball Players. International Journal of Sports Physiology & Performance, 16(3), 333–341.

Gabbett, T. J. (2020). The Training-Performance Puzzle: How Can the Past Inform Future Training Directions? Journal of Athletic Training (Allen Press), 55(9), 874–884.

Grow, N., & Shackleford, S. J. (2020). The Sport of Cybersecurity: How Professional Sports Leagues Can Better Protect the Competitive Integrity of Their Games. Boston College Law Review, 61(2), 474–521.

Henne, K. (2017). “I Felt Like a Lab Rat”: The Importance of Power and Context in Understanding Biometric Technologies. American Journal of Bioethics, 17(1), 63–65. https://doi-org.proxygsu-nga1.galileo.usg.edu/10.1080/15265161.2016.1251659

Jessop, A., & Baker III, T. A. (2019). Big Data Bust: Evaluating the Risks of Tracking NCAA Athletes’ Biometric Data. Texas Review of Entertainment & Sports Law, 20(1), 81–112.

Kaburakis, A., Rodenberg, R. M., & Holden, J. T. (2015, January 10). Inevitable: Sports gambling, state regulation, and the pursuit of revenue. https://www.hblr.org/2015/01/inevitable-sports-gambling-state-regulation-and-the-pursuit-of-revenue/.

Karkazis, K., & Fishman, J. R. (2017). Tracking U.S. Professional Athletes: The Ethics of Biometric Technologies. American Journal of Bioethics, 17(1), 45–60. https://doi-org.proxygsu-nga1.galileo.usg.edu/10.1080/15265161.2016.1251633

Khan, S., Parkinson, S., Grant, L., Na Liu, & Mcguire, S. (2020). Biometric Systems Utilising Health Data from Wearable Devices: Applications and Future Challenges in Computer Security. ACM Computing Surveys, 53(4), 85–85:29. https://doi-org.proxygsu-nga1.galileo.usg.edu/10.1145/3400030

Lazan, A., & Greenbaum, D. (2017). Collegiate Sports: Professionals All But in Name Raise Unique Bioethics Concerns in the Collection of Biometric Data. American Journal of Bioethics, 17(1), 70–72. https://doi-org.proxygsu-nga1.galileo.usg.edu/10.1080/15265161.2016.1251646

Li, R. T., Kling, S. R., Salata, M. J., Cupp, S. A., Sheehan, J., & Voos, J. E. (2016). Wearable Performance Devices in Sports Medicine. Sports Health: A Multidisciplinary Approach, 8(1), 74–78. https://doi-org.proxygsu-nga1.galileo.usg.edu/10.1177/1941738115616917

Osborne, B. (2017). Legal and Ethical Implications of Athletes' Biometric Data Collection in Professional Sport. Marquette Sports Law Review, 28(1), 37–84.

Rodenberg, R. M. (2021). Regulating Sports Gaming Data. UNLV Gaming Law Journal, 11(1), 9–90.

Smolenski, G. (2019). When the Collection of Biometric and Performance Data on College Athletes Goes Too Far. Wake Forest Law Review, 54(1), 279–301.

Studnicka, A. (2020). The Emergence of Wearable Technology and the Legal Implications for Athletes, Teams, Leagues and Other Sports Organizations Across Amateur and Professional Athletics, 16 DePaul J. Sports L. & Contemp. Probs. Retrieved from https://via.library.depaul.edu/jslcp/vol16/iss1/9

Williams, W. H. (2019). On the Clock, Best Bet to Draft Cyberdefensive Linemen: Federal Regulation of Sports Betting from a Cybersecurity Perspective. Brooklyn Journal of Corporate, Financial & Commercial Law, 13(2), 539–567.

Wixted, A. J., Thiel, D. V., Hahn, A. G., Gore, C. J., Pyne, D. B., & James, D. A. (2007). Measurement of Energy Expenditure in Elite Athletes Using MEMS-Based Triaxial Accelerometers. IEEE Sensors Journal, 7(4), 481–488. https://doi.org/10.1109/jsen.2007.891947