Florida State University Law Review

Volume 49 | Issue 1 Article 3

Fall 2021

Taboo Transactions: Selling Athlete Biometric Data

John T. Holden
Oklahoma State University

Kimberly A. Houser
University of North Texas

TABOO TRANSACTIONS: SELLING ATHLETE BIOMETRIC DATA

JOHN T. HOLDEN* AND KIMBERLY A. HOUSER**

ABSTRACT

As consumers begin to realize the extent to which their biometric and health data are being tracked through wearable devices, new privacy concerns have arisen. These concerns are more than hypothetical as the unregulated sharing and disclosure of biometric and health data may have serious repercussions. This is especially true for the athletes whose data is tracked with precision and where a lucrative market of multiple parties anxious to obtain this data already exists. The ownership and use of this data have become an incredibly complex issue, as sports leagues, teams, and the device makers wrangle over how this data should be used, shared, and potentially commercialized. Recent advances in data analytics have resulted in insights into athletic performance that a little over a decade ago were unimaginable. In Michael Lewis' Moneyball, *he described how Billy Beane, the General Manager of the Oakland A's, used advanced data analytics to build a winning baseball team. But biometric data promises even greater insight. This promise has made biometric data a priority across professional and amateur sports, however, it is not just teams and scouts with a major interest in this data, bookmakers and gamblers would also love to get access to this information. In light of the recent expansion of legalized sports gambling in the United States and the desirability of this information, we propose that measures need to be taken to protect the interests of professional athletes.*

We begin our examination by noting the sensitive nature of this type of data, which may include health, location, and performance information, requires the establishment of rules regarding how this data can be used with input from the players themselves. Currently, the use of this data may be controlled by the device maker or league rather than the athletes themselves. The concerns that the data collected from an athlete can be used against her in contract negotiations, made publicly available, discovered by competing teams through negligence or cyber-espionage, or by gamblers or bookmakers looking to gain an edge must be addressed. We then investigate the important issue of ownership. To

* John T. Holden is an Assistant Professor in the Spears School of Business at Oklahoma State University.

** Kimberly A. Houser is an Assistant Clinical Professor at the G. Brint Ryan College of Business at the University of North Texas. The authors would like to thank the participants at the 2020 Law and Ethics of Big Data Colloquium sponsored by Cecil B. Day Program for Business Ethics Machine Learning @ Georgia Tech (ML@GATECH), Georgia Institute of Technology, Scheller College of Business; The Department of Business Law and Ethics, Kelley School of Business at Indiana University, and Virginia Tech, Center for Business Intelligence and Analytics, Pamplin College of Business, for their helpful remarks.

what extent should the league or the device maker be able to profit from a player's athlete biometric data (ABD)? Not only do very few states have regulations addressing these issues, the current handling of ABD through bilateral agreements which do not include all stakeholders is insufficient. We conclude by proposing a new paradigm for addressing these concerns: Data Trusts.

INTRODUCTION

The wearable tech market is a growing part of the fitness industry, with more than eighty-five million smartwatches projected to be sold by the end of 2019, and sales expected to top $27 billion by 2022.[1] The intangibles tracked by wearable technology, however, promise to have even greater value than the wearables themselves.[2] This is especially true with respect to professional and collegiate athletes whose data is regularly used for training purposes, contract decisions, fantasy leagues, and sports betting. In fact, a cottage industry of biometric and movement tracking companies has emerged to provide a level of precision that is not necessary or required by ordinary consumers.[3]

In the wake of the Supreme Court's decision in *Murphy v. National Collegiate Athletic Association*,[4] which opened the doors for states to begin legalizing sports wagering, the value of athlete biometric data (ABD) has skyrocketed.[5] As the types of information and reports generated from the information becomes more sophisticated, so do the legal issues.[6] The COVID-19 pandemic only increased teams' reliance on

---

1. Paul Lamkin, *Smart Wearables Market to Double By 2022: $27 Billion Industry Forecast*, FORBES (Oct. 23, 2018, 8:04 AM), https://www.forbes.com/sites/paullamkin/2018/10/23/smart-wearables-market-to-double-by-2022-27-billion-industry-forecast/#5258df5f2656 [https://perma.cc/4NND-2FL3].

2. While the technology in Fitbit products and smartwatches, like the Apple Watch, are groundbreaking, the technology within products used by professional and elite athletes, like Whoop straps, provide greater precision and are designed for periodization and planning for future training, as opposed to tracking only past activity. *See* Erik Chen, *Whoop Strap 3.0 vs. Fitbit Inspire HR Review: A Product Analysis*, MEDIUM (Mar. 8, 2020), https://medium.com/age-of-awareness/whoop-strap-3-0-vs-fitbit-inspire-hr-review-a-product-analysis-995c58a633c5 [https://perma.cc/LE33-LMWZ].

3. The Whoop strap, for instance, is a wrist strap that is capable of measuring a variety of metrics, including heart rate variability, resting heart rate, and sleep patterns. The band is designed for individuals engaged in regimented training programs to tailor their training to maximize performance. *See* Mercey Livingston, *Whoop Strap 3.0 Review: A Great Fitness Tracker for High Performers and Serious Exercise Fans*, CNET (Feb. 11, 2020, 10:44 AM), https://www.cnet.com/health/whoop-3-0-review-a-great-fitness-tracker-for-high-performers-and-serious-exercise-fans/ [https://perma.cc/J5VK-R2FN].

4. 138 S. Ct. 1461 (2018).

5. John T. Holden, *The Major Issues Behind Biometric Data and Its Potential in Legal Sports Betting*, LEGAL SPORTS REP. (June 5, 2019), https://www.legalsportsreport.com/32915/biometric-data-legal-sports-betting/ [https://perma.cc/H9UC-VRCE].

6. The rise of legal gambling exposes a number of potential legal issues surrounding the use of biometric data, including who can use the data, for what purposes the data can be used, who can control the data, and how the data is to be stored. Historically, one of the greatest threats that athletes faced was in the form of individuals seeking to gain access to inside information regarding player injuries, as such, the abundance of new gambling opportunities may create an increased market for those who traffic in information and thus necessitate that leagues and athletes come to agreements of access, uses, and storage of biometric information. *See* Mike Florio, *Disclosure of Injury Information Continues to Put NFL Players in a Delicate Spot*, NBC SPORTS (July 10, 2015, 12:34 PM), https://profootballtalk.nbcsports.com/2015/07/10/disclosure-of-injury-information-continues-to-put-nfl-players-in-a-delicate-spot/ [https://perma.cc/F5AP-N8FV].

athletes training independently and using wearable technology to check in on athletes remotely.[7] As players, leagues, colleges, and the makers of wearables struggle with issues of privacy, data security, data use, data sharing, and the commercialization of data, scholars have recommended various solutions, primarily based on contract or intellectual property law.[8] However, these solutions fail to acknowledge how personal data exchanged for free services (such as in the case of Google or Facebook) differs from the legal issues arising from the collection and use of athletes' highly personal performance and health data 24/7. Nor does the current legal paradigm address the tricky ownership and sharing issues resulting from the use of data in sports betting. Unlike the way the United States treats personal data through a series of patchwork regulations that only protect certain types of data collected by certain types of entities from being shared without consent, we suggest a solution for the unique problems with ABD via the creation of a data trust for ABD. Rather than a model of ownership of ABD, we propose that a data trust can address what ownership seeks to resolve—namely controlling the use and addressing the risks in sharing data, as well as the ability to monetize the data. A data trust will allow fiduciary trustees to decide how the data can be used and with whom it can be shared. It is essentially a governance structure that can address the concerns of the multiple stakeholders in an agile way, providing a clear, legally accountable governance structure.

This Article is divided into six substantive parts. In Part I, we provide an overview of biometric data and its value in the world of sports. Part II discusses the issues surrounding data ownership in the major professional sports leagues and NCAA institutions. Part III examines the growth and importance of commercial data sales within athletic organizations and the implications for the athletes whose data is being collected. Part IV examines biometric data risks in privacy, employment, the integrity of data, data breaches, and theft. Part V analyzes the legal and ethical questions surrounding the ownership of this data.

---

7. *See, e.g.*, *Toronto FC Monitoring Athletes Remotely During COVID-19 (Part One)*, CATAPULT SPORTS (May 19, 2020), https://www.catapultsports.com/blog/toronto-fc-monitoring-athletes-remotely-during-covid-19-part-one [https://perma.cc/JNL9-RLVX] (noting that Toronto FC, a Major League Soccer team, was utilizing the catapult system to monitor players during the COVID-19 pandemic).

8. *See, e.g.*, Brian R. Socolow & Leuan Jolly, *Game-Changing Wearable Devices that Collect Athlete Data Raise Data Ownership Issues*, WORLD SPORTS ADVOC. (July 2017), https://www.loeb.com/en/insights/publications/2017/07/game-changing-wearable-devices-that-collect-athl__ [https://perma.cc/C9AL-DATL] (noting intellectual property issues and legal limitations on dissemination in both the United States and overseas). *See also* Barbara Osborne & Jennie L. Cunningham, *Legal and Ethical Implications of Athletes' Biometric Data Collection in Professional Sport*, 28 MARQ. SPORTS L. REV. 37, 59-65 (2017) (discussing the inclusion of biometrics collection within collective bargaining agreements across the major professional sports).

Part VI looks at how other countries approach biometric data collection and use and proposes a new model to clarify ownership rights and enhance the protection of ABD through contractual provisions.

I. TRACKING DATA

In the short time since the United States Supreme Court struck down a federal law in 2018, which largely confined sports gambling to the State of Nevada,[9] more than twenty states and the District of Columbia have passed laws allowing for sports betting within their borders.[10] One of the most contentious areas of this newly legal industry is the data that drives sportsbook offerings,[11] especially data collected from wearables.[12]

A. Overview of Gambling Market

Betting on sports is nearly as old as sport itself.[13] But, unlike in many countries across Europe and Asia,[14] sports betting was mostly illegal outside the confines of Nevada in the United States—the result

---

9. *See* Murphy v. NCAA, 138 S. Ct. 1461 (2018) (holding that the Professional and Amateur Sports Protection Act violated the anti-commandeering clause of the Constitution).

10. Ryan Rodenberg, *United States of Sports Betting: An Updated Map of Where Every State Stands*, ESPN (last updated June 1, 2020), https://www.espn.com/chalk/story/_/id/19740480/the-united-states-sports-betting-where-all-50-states-stand-legalization [https://perma.cc/SZQ3-GZ64].

11. Traditionally, sportsbooks have operated by offering betting on propositions that occur at the end of a game. *See* Brett Smiley, *The Rise and Excitement of In-Play Betting, Explained by an Expert*, SPORTS HANDLE (Dec. 13, 2017), https://sportshandle.com/in-play-sports-betting-expert-analysis/ [https://perma.cc/UA37-VEC4]. For instance, money-line wagers and point spread bets are those that are most often associated with the end scores of a game or do not rely on real-time data to determine the outcome. *See How to Bet on Sports – Guide to the Different Types of Wagers*, ONLINE GAMBLING SITES, https://www.onlinegamblingsites.com/betting/wagers-bets/ [https://perma.cc/SS4A-TCE4] . However, there has been a recent trend towards in-play wagering, which is wagering that occurs where a match is in progress. *See* Smiley, *supra* note 11. This type of wagering relies on high-speed transmission of data, which has created a market for companies that transmit this data. *Id.* Some have suggested that in-play wagering on propositions derived from athletes' biometric tracking is a future innovation in the sports betting market. *See* Jacob Gershman, *The Brave New World of Betting on Athletes' Data*, WALL ST. J. (Mar. 10, 2020), https://www.wsj.com/articles/the-brave-new-world-of-betting-on-athletes-data-11583848891 [https://perma.cc/RV9R-EBEX]; *see also* Holden, *supra* note 5.

12. *See* James Glanz & Agustin Armendariz, *When Sports Betting is Legal, the Value of Game Data Soars*, N.Y. TIMES (July 2, 2018), https://www.nytimes.com/2018/07/02/sports/sports-betting.html [https://perma.cc/R2QP-VK9U] (sports betting has expanded beyond who will win a match to what is known as in-play betting, such as who will score, who will assist, and where the ball will land).

13. John T. Holden, *Regulating Sports Wagering*, 105 IOWA L. REV. 575, 576 (2020).

14. *The Rise of Sports Betting Wagering Worldwide*, EUROPEAN BUS. REV. (Apr. 6, 2021), https://www.europeanbusinessreview.com/the-rise-of-sports-betting-wagering-worldwide/ [https://perma.cc/C6YH-ZCL9]; *see* Muralee Das, *Fantasy Sports and Gambling Regulation in the Asia-Pacific*, INT'L SPORTS L.J. 166, 175-76 (Aug. 5, 2021), https://link.springer.com/article/10.1007/s40318-021-00198-8 [https://perma.cc/KW3V-9C9U].

of a 1992 federal law[15] that froze state sports gambling laws in place.[16] America's prohibition on sports betting did not stop Americans from betting on sport; instead, Americans simply wagered illegally, driving a market estimated to have a value of $80-400 billion annually.[17] The tide began to turn in the United States with the rise of daily fantasy sports (DFS).[18] DFS games bear little resemblance to their season-long predecessors, which are typically played for small stakes amongst friends.[19] Instead, DFS contests are played with hundreds and even thousands of strangers for upwards of millions of dollars in prize money.[20]

While DFS was testing the American public's appetite for sports wagering out in the open, a nearly six-year legal fight would come to a head when the Supreme Court ruled that the Professional and Amateur Sports Protection Act (PASPA), which froze sports gambling laws in 1992, unconstitutionally commandeered state legislatures to maintain state laws to accomplish federal policy objectives.[21] Since the demise of PASPA, more than twenty states and the District of Columbia have legalized sports wagering.[22] With the rise of sports betting, there

15. 28 U.S.C. §§ 3701-3704 (1992).

16. The exact number of states with exemptions to offer some form of sports gambling is something of an unknown. Nevada, Montana, Delaware, and Oregon were the states who were operating sports betting contests of some value to the state and therefore were exempted, though only Nevada offered legal sportsbooks style wagering, which many conceive of when they hear the term sports betting. There is, however, evidence that other states like New Mexico had limited exemptions as well. *See* Ryan M. Rodenberg & John T. Holden, *Sports Betting Has an Equal Sovereignty Problem*, 67 DUKE L.J. ONLINE 1, 14-16 (2017).

17. Anastasios Kaburakis et al., *Inevitable: Sports Gambling, State Regulation, and the Pursuit of Revenue*, 5 HARV. BUS. L. REV. ONLINE 27, 28 (2015). There has been some skepticism about the upper estimates of the market, but few argue that the size of the illegal sports gambling market is not significant. *See* Jordan Weissmann, *Is Illegal Sports Betting a $400 Billion Industry?*, SLATE (Nov. 21, 2014), https://slate.com/business/2014/11/adam-silver-says-theres-400-billion-per-year-of-illegal-sports-betting-in-the-u-s-alone-seriously.html [https://perma.cc/7N7R-CUSU].

18. John T. Holden, *Prohibitive Failure: The Demise of the Ban on Sports Betting*, 35 GA. ST. U. L. REV. 329, 358-60 (2019).

19. *Id.* at 359.

20. John T. Holden et al., *Daily Fantasy, Tipping, and Wire Fraud,* 21 GAMING L. REV. 8, 9-10 (2017). A major change occurred when the *New York Times* published an op-ed by NBA commissioner Silver, who stated, "[i]n light of these domestic and global trends, the laws on sports betting should be changed. Congress should adopt a federal framework that allows states to authorize betting on professional sports, subject to strict regulatory requirements and technological safeguards." Adam Silver, *Legalize and Regulate Sports Betting*, N.Y. TIMES (Nov. 13, 2014), https://www.nytimes.com/2014/11/14/opinion/nba-commissioner-adam-silver-legalize-sports-betting.html [https://perma.cc/XPV2-TQYM].

21. Murphy v. Nat'l Collegiate Athletic Ass'n, 138 S. Ct. 1461, 1484-85 ("The legalization of sports gambling requires an important policy choice, but the choice is not ours to make. Congress can regulate sports gambling directly, but if it elects not to do so, each State is free to act on its own.").

22. *See* Dustin Gouker, *Legislative Tracker: Sports Betting*, LEGAL SPORTS REP., https://www.legalsportsreport.com/sportsbetting-bill-tracker/ [https://perma.cc/9K7D-ZMH4] (providing a list of states that have introduced legislation to legalize sports wagering).

has been an increase in pressure placed on state lawmakers to earmark money for professional sports leagues.[23] What began as a demand for an "integrity fee," or simply a private tax for offering wagers on a given sport,[24] transitioned into a mandate for sports betting operators to use official sports league data after the demand for a fee without anything in return appeared to be too brazen an ask.[25] Efforts to push for the use of official league data have been mostly unsuccessful, except with a limited requirement in Illinois, Tennessee, Virginia, and Michigan.[26] The commodification of sports gambling data is a multi-billion dollar business,[27] and both sports leagues and unaffiliated data brokers have been looking for ways to capitalize on the nascent U.S. sports gambling market.[28] The value of such information extends beyond the ability to offer unique types of betting propositions, to the ability for bookmakers and bettors to have access to even greater amounts of information to best inform their pricing or betting strategies.[29] Sports betting markets, like other markets, rely on information, and at present, there is a lack of clarity as to whether the athletes or team owners have the right to control the biometric information collected from players; this dispute creates uncertainty moving forward.[30]

B. What Is Biometric Data?

Sports teams have a long history of using data to evaluate players.[31] Today, sophisticated devices with sensors can be affixed to players to

---

23. *See* Brett Smiley, *Exclusive: Here's the 'Model' Sports Betting Playbook From NBA, MLB*, SPORTS HANDLE (Feb. 20, 2018), https://sportshandle.com/sports-betting-nba-mlb-model-act-integrity-fee/ [https://perma.cc/ZJ49-6BPF].

24. John T. Holden, *When They Say Integrity Fee, Are Pro Sports Leagues Really Asking For A Private Tax?*, LEGAL SPORTS REP. (Nov. 30, 2018), https://www.legalsportsreport.com/26361/pro-sports-leagues-integrity-fee-private-tax/ [https://perma.cc/53DP-4ARN].

25. John T. Holden & Mike Schuster, *The Sham of Integrity Fees in Sports Betting*, 15 N.Y.U. J.L. & BUS. 31, 37 (2020).

26. Becky Harris, *Federal Interference with State and Tribal Sports Betting Regulations Will Not Work: Where the Sports Wagering Integrity Act of 2018 Went Wrong and How Federal Legislation Might Be Effective*, 30 J. LEGAL ASPECTS SPORT 106, 129-30 (2020).

27. *See* Joe Vardon, *How MLB, the NBA, and the PGA Used 'Negotiation by Bayonet' to Get a Slice of the State Gambling Revenue*, ATHLETIC (Jan. 16, 2020), https://theathletic.com/1530989/2020/01/16/how-mlb-the-nba-and-the-pga-used-negotiation-by-bayonet-to-get-a-slice-of-state-gambling-revenue/ [https://perma.cc/T4WS-CJLG].

28. *See Official League Data*, LEGAL SPORTS REP., https://www.legalsportsreport.com/official-league-data/ [https://perma.cc/KB42-6RP6].

29. Holden, *supra* note 5.

30. *Id.*

31. *See generally*, Mike Pesca, *The Man Who Made Baseball's Box Score A Hit*, NPR (June 30, 2009), https://www.npr.org/templates/story/story.php?storyId=106891539 [https://perma.cc/8EUB-C6UD] (describing Henry Chadwick as the originator of the baseball box score, one of the first efforts to collect sports data).

collect data directly from them.[32] Although most are familiar with the Apple Watch and Fitbit, collegiate, amateur, and professional athletes use advanced wearables, such as the WHOOP Strap and the Catapult Sensor.[33] An athlete's biometric information consists of key indicators of health and performance. Both university and professional athletic programs have a long history of tracking performance data, including speed, reaction time, heart rate, body composition, strength.[34] Today's biometric wearable devices can collect over 1,000 data points per athlete per second.[35]

For the purposes of this Article, we will define athletic biometric data (ABD) as: "[a] measurable and distinguishable physical characteristic or personal behavioral trait used to recognize one's identity, including but not limited to name, nicknames, likeness, signatures,

---

32. *See* David Kravets, *How the NFL—Not the NSA—Is Impacting Data Gathering Well Beyond the Gridiron*, ARS TECHNICA (Sep. 1, 2019, 9:16 AM), https://arstechnica.com/tech-policy/2019/09/the-nfl-is-reshaping-the-surveillance-society-xbox-one-experience-and-gambling/ [https://perma.cc/XJ7B-HWPP]. These devices are connected to the internet and continually collect and analyze data in real-time in the device and at a remote server. The analysis may be viewed by the user or provided to third parties for their edification. Nicholas Zych, *Collection and Ownership of Minor League Athlete Activity Biometric Data by Major League Baseball Franchises*, 14 DEPAUL J. SPORTS L. 129, 131-33 (2018). This data collected from humans is measured or analyzed and is known as biometric data. Although biometrics were initially used to secure devices, such as requiring a fingerprint to access an iPhone or an iris scan to enter a secured location, today, data can be used to measure increasingly private information and monitor and predict future health conditions. This analysis happens in real-time, meaning information can be provided contemporaneously with the user's actions. *Id.*

33. *See* Brett Williams, *The Whoop Is Pro Sports' Favorite Wearable. After Training with It, I Can See Why*, MASHABLE (Dec. 21, 2017), https://mashable.com/2017/12/21/whoop-fitness-tracker-wearable-review/ [https://perma.cc/2SXY-8QLN]; Rainer Sabin, *Inside the Technology Giving Alabama a Competitive Edge*, AL.COM (July 2, 2017), https://www.al.com/alabamafootball/2017/07/inside_the_technology_giving_a.html [https://perma.cc/74KN-B2MX] (last updated Jan. 13, 2019). The Whoop strap has been called "the most powerful fitness tracker," it allows users to track their heart rates and activity strain in real-time, as well as enables the tracking of fatigue levels and sleep patterns. *See* Brett Williams, *There's Finally a Reason for You to Get a Whoop*, MEN'S HEALTH (Sept. 23, 2019), https://www.menshealth.com/fitness/a29076876/whoop-strap-3-review/ [https://perma.cc/AB65-Y6XG]. The Catapult sensor technology is capable of tracking more than one hundred different metrics, including an athlete's speed, acceleration, distance traveled, and heart rate. Mariam Sharia, *5 Amazing Pieces of Wearable Tech Being Implemented in Professional Sports*, WEARABLES (July 13, 2015), https://www.wearables.com/blogs/news/5-wearable-tech-pro-sports-micoach-zebra-catapult [https://perma.cc/QE55-CRA5].

34. George Foster et al., *Playing-Side Analytics in Team Sports: Multiple Directions, Opportunities, and Challenges*, FRONTIERS IN SPORTS & ACTIVE LIVING 9-11 (July 5, 2021), https://www.frontiersin.org/articles/10.3389/fspor.2021.671601/full [https://perma.cc/2URQ-VM6E].

35. Barbara Osborne & Jennie L. Cunningham, *Legal and Ethical Implications of Athletes' Biometric Data Collection in Professional Sport*, 28 MARQ. SPORTS L. REV. 37, 42 (2017). The NFL, for instance, has partnered with Zebra technology, which implants multiple trackers in every player's equipment. Other products, like STATS (of NBA data lawsuit fame) SportVU camera system, use missile-tracking technology to monitor ball and player movements, delivering a data stream that can be analyzed to provide information to coaches, agents, and gamblers.

pictures, activities, voice, statistics, playing and performance records, achievements, indicia, data, and other information identifying a particular athlete."[36]

The exact data being tracked depends on which device is employed.[37] There are now several biometrics tracking companies that provide various types of tracking.[38] The implementation of data-tracking devices is a huge advancement in understanding athlete performance and has been credited with providing significant improvements in understanding what training methods work best.[39] Among the most commonly used biometric tracking devices is Catapult.[40] Catapult is an Australian technology company that tracks movement based on a GPS sensor worn on an athlete's back.[41] More than 1,500 teams across thirty-five different sports use Catapult, including about half of the top college football teams in the United States.[42] Catapult is capable of tracking distance traveled by players and explosive plays and measurements of the physiological toll that plays take on a player.[43] In addition to the technology's ability to track data like an athlete's heart rate, GPS can also track their location.[44]

The WHOOP band is a wristband strap that continuously tracks an individual's heart rate, as well as their sleep patterns.[45] The technology, which has recently been made available to the recreational athlete, is capable of measuring heart rate and, via an algorithm, which determines the amount of "strain" a person has exerted in a given day.[46] The WHOOP band is touted for its ability to monitor trends, which can then measure workload and adjust training based on the individual athlete.[47] Other companies, like Nike and Under Armour,

---

36. Holden, *supra* note 5.

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

38. *Id.*

39. Shourjya Sanyal, *How Are Wearables Changing Athlete Performance Monitoring?*, FORBES (Nov. 30, 2018), https://www.forbes.com/sites/shourjyasanyal/2018/11/30/how-are-wearables-changing-athlete-performance-monitoring/#4a88e8d1ae09 [https://perma.cc/W4G2-MH3G].

40. Jessop & Baker, *supra* note 37.

41. *Id.*

42. *Id.*

43. Marc Tracy, *Technology Used to Track Players' Steps Now Charts Their Sleep, Too*, N.Y. TIMES (Sep. 22, 2017), https://www.nytimes.com/2017/09/22/sports/ncaafootball/clemson-alabama-wearable-technology.html [https://perma.cc/GCV3-6M7L].

44. *New Catapult Vector Integrates Indoor/Outdoor Tracking and Heart-Rate Monitoring in Vector Wearable*, GEO SPATIAL WORLD (Feb. 8, 2019), https://www.geospatialworld.net/news/new-catapult-vector-integrates-indoor-outdoor-tracking-and-heart-rate-monitoring-in-vector-wearable/ [https://perma.cc/G4M5-X85S].

45. Jessop & Baker, *supra* note 37.

46. Julia Malacoff, *I Tried the Fanciest Fitness Tracker on the Market*, SHAPE, https://www.shape.com/fitness/gear/whoop-fitness-tracker-review-workout-recovery-features [https://perma.cc/L7UZ-AL2J].

47. Jessop & Baker, *supra* note 37, at 88.

are trying to capture part of the tracking market, with both apparel giants carving out deals with colleges to track activity-based information including: "speed, distance, vertical leap height, maximum time aloft, shot attempts, ball possession, heart rate, running route, etc."[48]

C. *Why Is It Tracked?*

According to scholars Osborne and Cunningham, who have studied the reasons for implementing biometric tracking programs:

> The most common reasons [for tracking biometric data] are to monitor a player's health, wellness, and performance; establish baselines, perform diagnostics, understand player load, educate coaches (and players) on the effects of training on players; and to design appropriate training and recovery regimens—key priorities are to develop the players, prevent and monitor injuries, and injury rehabilitation.[49]

However, recent advances in data analytics have resulted in novel insights into athletic performance that a little over a decade ago were unimaginable. In Michael Lewis' *Moneyball*, Lewis describes how Billy Beane, the General Manager of the Oakland A's, used advanced data analytics to build a winning baseball team in the early 2000s.[50] Beane hired a Harvard economics graduate to conduct analytics on data collected, such as when a player was drafted, finding, for example, that players drafted out of college performed better than those drafted out of high school.[51] Additionally, "sabermetrics," a term for advanced baseball statistics, could make more accurate predictions than the scouts and managers about a player's future performance based on past performance.[52] Initially, many were skeptical of this method because "gut instinct" was considered the best measure of future

---

48. *Id.* at 89.

49. *See* Osborne & Cunningham, *supra* note 35, at 40.

50. By removing unconscious biases from player selection and relying more on data, the Oakland A's dramatically improved the team's performance while having the lowest payroll in their division. *See* MICHAEL LEWIS, MONEYBALL: THE ART OF WINNING AN UNFAIR GAME 270 (2003). For the benefits of artificial intelligence analytics to reduce unconscious bias, see Kimberly A. Houser, *Can AI Solve the Diversity Problem in the Tech Industry? Mitigating Noise and Bias in Employment Decision-Making*, 22 STAN. TECH. L. REV. 290, 324-331 (2019). Similarly, in baseball, players were chosen on how well they fit the stereotype of a great baseball player, height and appearance, rather than measurable skills, much like how employees are promoted based on if they fit the stereotype of a great manager, white and male, rather than measurable skills. *See* LEWIS, *supra* note 50, at 3-6.

51. LEWIS, *supra* note 50, at 16-18; *see* Richard Feloni, *'Moneyball' Author Michael Lewis Explains Why Professional Sports Teams Need to Reinvent the Role of Scouts*, BUS. INSIDER (Dec. 30, 2016, 12:50 PM), https://www.businessinsider.com/moneyball-michael-lewis-pro-sports-scouts-need-to-evolve-2016-12 [https://perma.cc/8TU9-LE6M].

52. *See generally* Ben Harris, *A Sabermetric Primer: Understanding Advanced Baseball Metrics*, ATHLETIC (Feb. 28, 2018), https://theathletic.com/255898/2018/02/28/a-sabermetric-primer-understanding-advanced-baseball-metrics/ (explaining advanced statistics commonly used in baseball) [https://perma.cc/WZY9-BH6Y].

performance.[53] Today, most sports teams use analytics in player selection.[54] While *Moneyball*-type analytics involves using data such as foot speed, batting average, and fastball velocity, the data available with modern-day wearables makes these data points seem antiquated.

D. What Is the Value?

Biometric data has enormous value for many reasons. One can infer much from Google's willingness to pay $2.1 billion for the biometric company FitBit.[55] As the analytics used on ABD advances, teams can predict future performance, better identify whom to recruit, and which players need a different health/training regime. There is a benefit to both the players and the teams in keeping players healthy and injury-free. As such, monitoring players' health has become de rigueur. The concern in this is that parties could use this information in contract negotiations, trade decisions, and other ways that the athlete was not expecting and may not desire.[56] While a lot of the information collected is performance-related, much of it is also health-related. The law treats personal health information (PHI) differently from non-health information.[57] Due to the nature of the data collected by wearables, there is no clear demarcation between PHI and other performance-related data. There is also uncertainty with respect to the ownership of the data.[58] The question then becomes, how do we monetize ABD while

53. Feloni, *supra* note 51.

54. *Id.*

55. Patrick Lucas Austin, *The Real Reason Google Is Buying Fitbit*, TIME (Nov. 4, 2019, 3:17 PM), https://time.com/5717726/google-fitbit/ [https://perma.cc/ZE6E-2PMM]. Reportedly, Google has already been collecting health information on millions of Americans through its partnerships with one of the nation's largest health care providers. Richard Nieva, *Google Reportedly Collects Health Data on Millions of Americans Without Informing Patients*, CNET (Nov. 11, 2019, 5:37 PM), https://www.cnet.com/news/google-reportedly-collecting-health-data-on-millions-of-americans-without-informing-patients/ [https://perma.cc/UE8V-V9DH]. Known as Project Nightingale, Google has already collected information such as lab results and hospitalization records. Although this partnership raises both ethical and legal concerns, the company insists that HIPAA permits such activities. Rebecca Robbins & Casey Ross, *HHS to Probe Whether Google's 'Project Nightingale' Followed Federal Privacy Law*, STAT (Nov. 13, 2019), https://www.statnews.com/2019/11/13/hhs-probe-google-ascension-project-nightingale/ [https://perma.cc/K4RT-SW3W].

56. Osborne & Cunningham, *supra* note 35, at 61; *see also* Jessica L. Roberts et al., *The Legality of Biometric Screening of Professional Athletes*, 17 AM. J. BIOETHICS 65, 65 (2017) ("Several aspiring professional athletes have seen their careers cut short by biometric screening. In 2013, Star Lotulelei's status in the National Football League (NFL) draft plummeted following an irregular electrocardiogram. Likewise, in 2014, Isaiah Austin withdrew from the National Basketball Association (NBA) draft after being diagnosed with Marfan syndrome. And in 2016, three NFL hopefuls—Jaylon Smith, Myles Jack, and Reggie Ragland—all ended up second-round draft picks due to suspected medical problems.") (internal citations omitted).

57. *See infra* Section V.A.

58. Holden, *supra* note 5.

also protecting it from undesirable uses? While some scholars have called for a model of data ownership,[59] others promote the creation of a privacy protection model.[60]

The value of the ABD does not generally stem from its existence in raw form, especially in a single data point, such as a football player's heart rate at 8:30 p.m. on a Monday night. Rather, the value stems from what one could infer from the data and therefore, about the player, and ostensibly, the team. Additionally, analytics that run on data collection points from multiple sources can provide a great deal of knowledge about a player, even data that the athlete is unaware of personally. The data created from these analytics is known as "derived data"; it presents additional risks to the player,[61] and in many cases the team, depending on who has access to this new derived data that is of value to many in and outside of the team.[62] It is not just players, scouts, coaches, team doctors, and owners that desire this data, or rather the predictions they can make from the derived data—researchers, fans, sportswriters, fantasy league players, and those who place sporting bets also obtain value from the derived data.

---

59. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 122–35 (1999); Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1, 4 n.15 (2018) (citing Louisa Specht, *Ausschließlichkeitsrechte an Daten—Notwendigkeit, Schutzumfang, Alternativen: Eine Erläuterung des gegenwärtigen Meinungsstands und Gedanken für eine zukünftige Ausgestaltung*, COMPUTER UND RECHT 288, 296 (May 2016) (Ger.) (discussing exclusivity rights to data—need, scope, and alternatives)); Karl-Heinz Fezer, *Dateneigentum der Bürger: Ein originäres Immaterialgüterrecht sui generis an verhaltensgenerierten Informationsdaten der Bürger*, BEITRÄGE 99, 99 (Mar. 2017) (Ger.); Václav Janeček, *Ownership of Personal Data in the Internet of Things*, 34 COMPUTER L. & SEC. REV. 1039, 1039 (2018); Kenneth C. Laudon, *Markets and Privacy*, COMMC'N ACM 92, 101 (Sept. 1996); Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63 (1999); Tom C.W. Lin, *Executive Trade Secrets*, 87 NOTRE DAME L. REV. 911, 968 (2012); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 11, 26-41 (1996); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2381-83 (1996); James B. Rule, *Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions*, 54 U. TORONTO L.J. 183, 185 (2004); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2056 (2004); Catherine M. Valerio Barrad, *Genetic Information and Property Theory*, 87 NW. U. L. REV. 1037, 1062-63 (1993); Herbert Zech, *A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data*, 11 J. INTELL. PROP. L. & PRAC. 460, 460-70 (2016). *But see* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1129 (2000) ("A property rights model for protecting personal data nevertheless presents many problems."). *See also* Jane B. Baron, *Property as Control: The Case of Information*, 18 MICH. TELECOMM & TECH L. REV. 367-418 (2012); Jamie Lund, *Property Rights to Personal Information*, 10 NW. J. TECH. & INTELL. PROP. 1, 1-18 (2011).

60. Determann, *supra* note 59, at 4; Jorge L. Contreras, *The False Promise of Health Data Ownership*, 94 N.Y.U. L. REV. 624, 624 (2019).

61. As more fully discussed in Part V, derived data are the inferences and reports created from the data collected through data analytics. *See infra* Part V.

62. ROB KITCHIN, THE DATA REVOLUTION: BIG DATA, OPEN DATA, DATA INFRASTRUCTURES & THEIR CONSEQUENCES 1 (Robert Rojek ed., 2014) (defining derived data as data produced from other data).

II. UNCERTAIN LEGAL STATUS OF DATA

Efforts to control sports information in the United States date back nearly a century, and perhaps even longer.[63] Much of sports league efforts to commodify their products in recent years have centered on broadcast rights to games and merchandising league and team intellectual property.[64] Professional leagues have occasionally pursued efforts to expand the range of products and information which they can control.[65] Sports leagues have tried both legislative[66] and judicial routes to expand the scope of protection for information and products arising from the existence of underlying sporting events.[67] Sports leagues have taken steps in recent years to compile data that cannot be easily replicable by spectators in the stands or viewers at home.[68] The NBA has introduced the SportVU camera system that uses missile tracking technology to determine player and ball movements during a game.[69] Major League Baseball has implemented the Statcast system, which is capable of tracking distance, launch angle, and flight path of baseballs after a batter strikes them, as well as player movements on the field.[70] Traditionally, these have just been complementary additions to television broadcasts, providing additional information that announcers can discuss and stat aficionados can use.[71] The major

63. *See, e.g.*, Pittsburgh Athletic Co. v. KQV Broad. Co., 24 F. Supp. 490, 493-94 (W.D. Pa. 1938) (holding "[t]he right, title and interest in and to the baseball games played within the parks of members of the National League, including Pittsburgh, including the property right in, and the sole right of, disseminating or publishing or selling, or licensing the right to disseminate, news, reports, descriptions, or accounts of games played in such parks, during the playing thereof, is vested exclusively in such members.").

64. Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 843-44 (2d Cir. 1997); *see also* C.B.C. Distrib. & Mktg., Inc. v. Major League Baseball Advanced Media, L.P., 505 F.3d 818, 820 (8th Cir. 2007).

65. *See* John T. Holden, *Making Sense Of Pro Sports Leagues' Search For Sports Betting Data Fees*, LEGAL SPORTS REP. (June 18, 2018), https://www.legalsportsreport.com/21245/search-for-sports-betting-fees/ [https://perma.cc/BGS3-E79Z].

66. *See, e.g., Legislation Prohibiting State Lotteries from Misappropriating Professional Sports Service Marks, Hearing Before the Subcomm. on Patents, Copyrights and Trademarks of the Committee on the Judiciary on S. 1772*, 101st Cong. 114 (1990) (featuring testimony of former NFL commissioner Paul Tagliabue testifying that while he was "not an expert on intellectual property law," he believed that the NBA was within its rights to assert a claim against the Oregon lottery who sought to allow wagering on NBA games).

67. *See Motorola*, 105 F.3d at 843-44.

68. Holden, *supra* note 65.

69. *Id.*

70. *Id.*

71. Data providers have recently entered into partnerships with leagues like Major League Baseball, gaining access to Statcast data in an effort to develop new products for consumers. *See Major League Baseball and Sportradar Announce Official Exclusive Global Partnership*, SPORTRADAR (Feb. 27, 2019), https://sportradar.us/2019/02/major-league-baseball-and-sportradar-announce-official-exclusive-global-partnership/ [https://perma.cc/M8CA-3ML8].

professional sports leagues in the United States are, however, preparing for a future where data does not just provide entertainment value, but becomes a commodity in itself.[72]

A. *Disputes Over Sport Data Ownership*

In 1972, a St. Louis Cardinals player, Curt Flood, argued that professional baseball's reserve system was an unconstitutional form of slavery in that the team essentially owned players due to the team's ability to renew a player's contract continuously.[73] Although Flood lost this case,[74] it would lead to the creation of the concept of "free agency," eliminating the player as a property right issue.[75] Under the former system, players were "reserved" for the team with which they played and had no right to negotiate with another team.[76] Due to collective bargaining agreements, players today cannot be traded without their consent and have free agency rights.[77] Later cases addressed the ownership issues of sports data.[78] While the leagues attempted to prevent commercial entities from selling data (such as access to sports scores) to the public, courts have uniformly denied these cases as there can be no ownership of facts under U.S. copyright law.[79] Sports leagues have been attempting to control access to the information generated by sporting events for decades.[80]

In 1990, the NBA brought suit against Motorola and the company STATS over sales of a pager system that provided users with scores of NBA games at various intervals.[81] The NBA argued that the Defendants were freeriding on the NBA's labor, but the Second Circuit held that Motorola was gathering information at its own costs; it was not simply copying the NBA's reporting of game information, and thus did

---

72. Holden, *supra* note 5.

73. Flood v. Kuhn, 407 U.S. 258, 258-59 (1972).

74. *Id.* at 282 (relying on Fed. Baseball Club of Balt., Inc. v. Nat'l League of Prof'l Baseball Clubs, 259 U.S. 200 (1922)).

75. Allen Barra, *How Curt Flood Changed Baseball and Killed His Career in the Process*, ATLANTIC (July 12, 2011), https://www.theatlantic.com/entertainment/archive/2011/07/how-curt-flood-changed-baseball-and-killed-his-career-in-the-process/241783/ [https://perma.cc/J6FM-7YZL].

76. *Id.*

77. *Id.*

78. *See* Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 843-44 (2d Cir. 1997); *see also* C.B.C. Distrib. & Mktg., Inc. v. Major League Baseball Advanced Media, L.P., 505 F.3d 818, 820 (8th Cir. 2007).

79. Nat'l Football League v. Governor of Del., 435 F. Supp 1372, 1391 (D. Del. 1977) (holding that Delaware lottery is permitted to reproduce schedules and scores); *Motorola*, 105 F.3d at 855 (holding that Motorola is permitted to sell handheld device displaying basketball scores in real-time).

80. Holden, *supra* note 24.

81. *Motorola*, 105 F.3d at 843-44.

not satisfy the elements of hot news misappropriation.[82] The court rejected the NBA's hot news claim, as well as the league's claim that Motorola had infringed on league copyrights.[83] In 2007, Major League Baseball's licensing arm would make a similar argument regarding ownership of the protection of information generated by a baseball game by the right of publicity.[84] The court in *C.B.C. Distribution & Marketing, Inc. v. Major League Baseball Advanced Media* held that the First Amendment protects player statistics, names, and game results, thus trumping any right of publicity claims by Major League Baseball Advanced Media.[85]

While sports leagues have historically sought to gain greater control over statistics and data than courts have allowed, biometric data may raise a different argument for sports leagues, as this information cannot be independently collected by an observer on television or in the stands.[86] There is, however, the potential for dispute in some sports leagues over who gets control of biometric data and what it can be used for, as few leagues appear to have considered the potential tension that biometric data would create between unions and league ownership.[87] Some start-up leagues have already built biometric data into their data sales plans, with more established leagues also beginning to explore the commercial use of biometric data.[88]

---

82. *Id.* at 852 (According to the Second Circuit, the elements of a hot news claim are: 1) "[T]he plaintiff generates or collects information at some cost or expense"; 2) "the value of the information is highly time-sensitive"; 3) "the defendant's use of the information constitutes free-riding on the plaintiff's costly efforts to generate or collect it"; 4) "the defendant's use of the information is in direct competition with a product or service offered by the plaintiff"; and 5) "the ability of other parties to free-ride on the efforts of the plaintiff would so reduce the incentive to produce the product or service that its existence or quality would be substantially threatened.").

83. *Id.* at 847 ("Although the broadcasts are protected under copyright law, the district court correctly held that Motorola and STATS did not infringe NBA's copyright because they reproduced only facts from the broadcasts, not the expression or description of the game that constitutes the broadcast.").

84. *See* C.B.C. Distrib. & Mktg., Inc. v. Major League Baseball Advanced Media, L.P., 505 F.3d 818, 820 (8th Cir. 2007).

85. *See id.* at 824 ("Because we hold that CBC's first amendment rights in offering its fantasy baseball products supersede the players' rights of publicity, we need not reach CBC's alternative argument that federal copyright law preempts the players' state law rights of publicity.").

86. Holden, *supra* note 5.

87. *See generally* Kristy Gale, *Evolving Sports Technology Makes Its Mark on the Internet of Things: Legal Implications and Solutions for Collecting, Utilizing, and Disseminating Athlete Biometric Data Collected Via Wearable Technology*, 5 ARIZ. ST. U. SPORTS & ENT. L.J. 337, 364-69 (2015).

88. Adam Candee, *Key Questions Raised By Report MGM-AAF Sports Betting Deal*, LEGAL SPORTS REP. (Sep. 10, 2018), https://www.legalsportsreport.com/23963/mgm-aaf-sports-betting-deal/ [https://perma.cc/N5KS-QT3U].

B. League Versus Player Association Claims to Biometric Ownership

At the 2019 Sports Lawyers Association Conference, biometric data tracking was one of the topics of discussion amongst panels featuring representatives from the four prominent American sports leagues, as well as their respective players' associations.[89] Three of the four major sports leagues have limited agreements in place with their players regarding the collection of biometric data: the NFL has only a basic template in place and is planning to revisit the subject during future collective bargaining negotiations;[90] the NHL's agreement with the Players' Association allows for some commercial sales of agreed-upon biometric data; Major League Baseball's agreement with the Players' Association does not allow for the commercialization of the data, and players remain free to opt out of the tracking program.[91]

While the future permissible uses of professional ABD in organized team sports is likely to be determined via the collective bargaining process, at present, three of the four leagues and players' associations are still in nascent stages of crafting their policies governing the collection, use, and sales of ABD.[92] The dispute over wearables and biometric tracking technology comes from fears that parties might utilize the data against a player's interests.[93] What undoubtedly started as a well-intentioned means of tracking player health, now has potential consequences that can result in players being deemed unsuitable for the league or players receiving smaller contract offers as a result of biometric observations.

III. PROFESSIONAL LEAGUES AND DATA SALES

The sale of sports rights has been one the most lucrative aspects of the commercialization of sport in the United States. While the sale of broadcast rights has long been held up as the pinnacle of sport monetization with multi-billion-dollar contracts becoming the norm,[94] other property rights sales are beginning to approach the value of television

89. Holden, *supra* note 5.

90. *Id.*

91. *Id.*

92. Kristy Gale, *The Sports Industry's New Power Play: Athlete Biometric Data Domination. Who Owns It and What May Be Done with It?*, 6 ARIZ. ST. U. SPORTS & ENT. L.J. 7, 74-77 (2016) (discussing how athletes can control the dissemination of biometric data via collective bargaining).

93. In addition to the privacy and commoditization issues, athletes fear that their ABD could be used against them in contract negotiations. Jeremy Venook, *The Upcoming Privacy Battle Over Wearables in the NBA*, ATLANTIC (Apr. 10, 2017), https://www.theatlantic.com/business/archive/2017/04/biometric-tracking-sports/522222/ [https://perma.cc/2M4E-36YJ].

94. *See* Brad Adgate, *The Sports Bubble Is Not Bursting*, FORBES (Jan. 16, 2018, 9:34 AM), https://www.forbes.com/sites/bradadgate/2018/01/16/the-sports-bubble-is-not-bursting/#9c5e8b63bba3 [https://perma.cc/J374-Q9C8].

contracts.[95] The more information that sports leagues can bundle into data packages to sell, the more valuable those packages will likely be.[96] This Part explains how data is currently being used.

A. Professional League Structures

With the advent of legal sports betting in the United States, sports league data has fast become one of the most valuable assets for professional sports leagues.[97] The major professional team sports leagues in the United States have a monopoly for their respective sports.[98] Osborne and Cunningham have noted, "Professional sports are characterized by a unique labor structure: (1) an anti-competitive system maintained to preserve competition; (2) players' associations bargain for contract terms binding on all players; and (3) athletes, unlike employees in other industries, are inherently elite, temporary, and relatively replaceable—but necessary to the very existence of pro sports."[99] Individual professional teams contract with players and negotiate salaries. Other working conditions and terms of employment, however, such as salary caps, are subject to cóllective bargaining between the team owners, represented by the league, and the players represented by their union players' association.[100] The collection of biometric data, as well as the sale and any restrictions on its use, is almost certain to be subject to the collective bargaining process for the four major professional sports leagues in the future.[101]

---

95. Leagues have begun diversifying their offerings, offering streaming services and other products to consumers over the internet, as opposed to the traditional broadcast mediums. Andrew Cohen, *NBA TV Launches Its Own Subscription Streaming Channel*, SPORTTECHIE (Nov. 5, 2019), https://www.sporttechie.com/nba-tv-subscription-streaming-channel. Data sales may well become as lucrative as broadcast television contracts, especially as more consumers abandon traditional cable television for a la cart streaming preferences. *See* Wayne Perry, *Leagues Finally Cash In on Sports Betting by Selling Data*, AP (Jan. 7, 2020), https://apnews.com/2fc27b7c558ceddd8669fb03acc15e3d [https://perma.cc/Q733-MTL4].

96. *See* John Holden, *Can Leagues Own Data Rights When It Comes to US Sports Betting?*, LEGAL SPORTS REP. (May 29, 2018), https://www.legalsportsreport.com/20745/leagues-and-fees-in-sports-betting/ [https://perma.cc/G9WQ-285H].

97. *See* Luke Massey, *The US Sets "New Benchmark" For Extracting Value from Sports Betting*, SBC NEWS (Apr. 24, 2019), https://www.sbcnews.co.uk/features/2019/04/24/us-new-benchmark-extracting-value-sports-betting/ [https://perma.cc/HWE4-6A86].

98. John T. Holden & Thomas A. Baker III, *The Econtractor? Defining the Esports Employment Relationship*, 56 AM. BUS. L.J. 391, 401 (2019). The four major leagues operate as a joint venture between league management and franchise owners, operating in cities across the continent. *Id.*

99. Osborne & Cunningham, *supra* note 35, at 58-59 (footnotes omitted).

100. Holden & Baker, *supra* note 98.

101. Chris Hoffman, *Seventh Circuit Suggests that Unions Can Negotiate Workers' Biometric Data Privacy Rights with Employers*, AM. BAR. ASS'N (Aug. 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/cyberspace/2019/201908/unions/ [https://perma.cc/4H55-WAPJ]; *see* Gale, *supra* note 92 (discussing collective bargaining); *see also* Miller v. Southwest Airlines Co., 926 F.3d 898, 900 (7th Cir. 2019) (holding fingerprint collection is a subject to union consent).

B. Current Collective Bargaining Agreements

In March of 2017, Major League Baseball approved the use of the WHOOP strap during games.[102] In an attachment to the Major League Baseball's 2017-2021 collective bargaining agreement with the Players' Association, a player's use of wearable tracking is deemed voluntary.[103] Additionally, the agreement prohibits any commercial use of the data, limiting any opportunity to capitalize financially on the inclusion of biometric data as part of a data rights package.[104] The NBA's collective bargaining agreement was renewed at the same time as Major League Baseball's and similarly addressed wearable technology and what could be done with the data collected.[105] Section 13 of Article XXII of the NBA collective bargaining agreement sets out a mechanism for the creation of a joint NBA and Players Association committee to govern the approval of wearable tracking technology.[106] Like Major League Baseball, NBA players' participation in a wearables program is strictly voluntary and may be discontinued at any time.[107] In addition to wearables not being allowed during games, the NBA's collective bargaining agreement also prohibits the commercial sale of the data.[108]

In 2017, the NFL Players' Association reached an agreement with WHOOP to provide all players with a strap.[109] Under this agreement, players control their individual data.[110] While the Players' Association does not have an agreement with owners governing the use of ABD, the Players' Association has announced plans to include access to the

---

102. Will Ahmed, *WHOOP Approved for In-Game Use in Major League Baseball,* WHOOP (Mar. 6, 2017), https://www.whoop.com/the-locker/whoop-approved-for-in-game-use-in-major-league-baseball/ [p https://perma.cc/9V4D-ZXK9].

103. 2017-2021 Basic Agreement, Major League Baseball Players 1, 334 (2017), https://d39ba378-ae47-4003-86d3-147e4fa6e51b.filesusr.com/ugd/b0a4c2_958836906273 49e0a5203f61b93715b5.pdf [https://perma.cc/8HL9-W5TP].

104. *Id.* at 335. Notably, Minor league baseball players are not subject to the collective bargaining agreement. *See* Nicholas Zych, *Collection and Ownership of Minor League Athlete Activity Biometric Data by Major League Baseball Franchises,* 14 DEPAUL J. SPORTS L. 129, 132 (2018) (noting that minor league baseball players are not part of the Major League Baseball Players' Association and not parties to the professional league's collective bargaining agreement).

105. NBA–NBPA Collective Bargaining Agreement, NBPA 1, 359-61 (2017), https://cosmic-s3.imgix.net/3c7a0a50-8e11-11e9-875d-3d44e94ae33f-2017-NBA-NBPA-Collective-Bargaining-Agreement.pdf [https://perma.cc/RAH3-572B].

106. *Id.* at 359-60.

107. *Id.* at 360.

108. *Id.* at 361.

109. Jared Dubin, *NFLPA Reaches Agreement to Provide Players with Biometric Monitors,* CBS SPORTS (Apr. 24, 2017, 10:31 AM), https://www.cbssports.com/nfl/news/nflpa-reaches-agreement-to-provide-players-with-biometric-monitors/ [https://perma.cc/JM5Y-LBMH].

110. *Id.*

data as part of the organization's licensing program.[111] NFL general counsel, Adolpho Birch III, opined that the 2020 collective bargaining negotiations likely will include a discussion over the collection and dissemination of ABD.[112]

The NHL, which has a partnership with tracking company Catapult,[113] does not have a wearables policy within the current collective bargaining agreement, which runs through 2022.[114] With no agreement in place, the union and ownership appear to be on different pages as to what to do with the data, with ownership looking to the commercial value and the union seeking to protect players' privacy.[115] Despite the lack of agreement, the NHL has begun making certain player tracking and puck movement data available commercially.[116]

The commercialization of player tracking data is new, and it appears to be growing rapidly. The Australian Football League and the Professional Squash Association are both selling real-time player tracking data to interested buyers,[117] and the now-defunct Alliance of American Football, built part of their data rights package around biometric and player tracking data.[118] However, the nascent legal sports gambling industry has spurred the need to address the legal issues raised by ABD collection.[119]

C. Desirability of Biometric Data to Gambling Entities

The agreement between the Alliance of American Football and MGM gaming was the first of its kind in North America.[120] The MGM deal provided for the casino giant to collect the data in real-time from the field, and using an algorithm, create new betting odds based on the

111. Eric Fisher, *Data in Motion*, SPORTS BUS. DAILY (Oct. 22, 2018), https://www.sportsbusinessdaily.com/Journal/Issues/2018/10/22/In-Depth/Wearable-tech.aspx [https://perma.cc/P3VQ-P2WG].

112. Holden, *supra* note 5.

113. Greg Wyshynski, *Player Tracking Coming to the NHL? It's Complicated*, ESPN (Feb. 28, 2018), https://www.espn.com/nhl/story/_/id/22604597/nhl-great-player-tracking-debate-ethical-questions-fan-access [https://perma.cc/C28X-BPV2].

114. Osborne & Cunningham, *supra* note 35, at 64.

115. Wyshynski, *supra* note 113.

116. Holden, *supra* note 5.

117. Fisher, *supra* note 111.

118. Joe Lemire, *Alliance of American Football Is Betting on Data to Grow New League*, SPORTTECHIE (Oct. 9, 2018), https://www.sporttechie.com/alliance-american-football-charlie-ebersol-bill-polian/ [https://perma.cc/S4ZP-LRET].

119. *See* Brant James, *Biometrics: Currency, Conundrum in Sports Betting Future*, GAMBLING.COM (Nov. 30, 2018), https://www.gambling.com/news/biometrics-currency-conundrum-in-sports-betting-future-1693000 [https://perma.cc/M8PM-Q4Z9].

120. Derek Blake, *Is Biometric Data the New Frontier in Sports Betting*, WSN (June 7, 2019), https://www.wsn.com/betting/biometric-data-new-frontier-sports-betting/ [https://perma.cc/E9EG-EKEB].

information recorded.[121] The value to gambling operators is more than having information that is not widely available, but there is also the potential to offer new betting options that might draw in additional customers.[122] While start-up leagues like the Alliance of American Football are being built around gambling, the four major leagues' players' associations have all expressed some concern about ABD being accessible to gamblers.[123] Yet, despite the current resistance to including biometric data in data rights packages, as data sales become more lucrative sportsbook operators are likely to begin seeking additional types of data—data that is proprietary.[124] Kristy Gale, an expert on sports technology, stated: "Sports betting is pushing the envelope because it's the biggest moneymaker, and it is one of the biggest ways, if not the biggest way, to engage fans in a game in real time."[125]

Sports leagues and data providers are seeking to create value as the American market begins to take shape, and one of the ways that leagues are creating unique products is by including data in their packages that cannot be easily replicable without consent of the league.[126] The terms of many of the US-based data deals remain confidential, but the NBA's $250 million deal with Sportradar to distribute gambling data overseas in 2016 is likely on the low end of the value of the most contemporary data deals.[127] While some have voiced concerns about athletes' privacy rights, others see the use and licensing of player biometric data as an untapped revenue stream for player publicity rights, capable of creating more value than ever before for high-level athletes.[128] One of the difficulties is that there is a growing demand for advanced statistics, and there is a "difficulty in differentiating [biometric health data] from game data."[129]

---

121. *Id.*

122. *See* Andy Rosen, *Should Gamblers See Athletes Heart Rates During Games?*, BOS. GLOBE (June 5, 2019, 6:51 PM), https://www.bostonglobe.com/metro/2019/06/05/should-gamblers-see-athletes-heart-rates-during-games-hydration-indicators-their-sweat/jRZT9ZdaUQtqjEYCerzjeL/story.html [https://perma.cc/BR4E-RPG2].

123. *Id.*

124. *Id.*

125. *Id.*

126. *See* Brett Smiley, *MLB, Sportradar Ink Sports Betting Data Deal as Controversy Brews*, SPORTS HANDLE (Feb. 27, 2019), https://sportshandle.com/mlb-sportradar-announce-betting-data-deal/ [https://perma.cc/4GJW-PMDC].

127. Eben Novy-Williams, *NFL Takes First Major Gambling Step with Sportradar Data Deal*, BLOOMBERG (Aug. 12, 2019, 7:45 AM), https://www.bloomberg.com/news/articles/2019-08-12/nfl-takes-first-major-gambling-step-with-sportradar-data-deal [https://perma.cc/YEN5-SV5U].

128. *How Biometrics in Sports Betting will Protect Intellectual and Publicity Rights*, YOGONET (July 6, 2018), https://www.yogonet.com/international/noticias/2018/07/06/47110-how-biometrics-in-sports-betting-will-protect-intellectual-and-publicity-rights?amp [https://perma.cc/2G5Z-E3Q9].

129. James, *supra* note 119.

There is nothing inherently nefarious about teams wanting to track ABD. Indeed, the health benefits derived from the information gathered by wearables are likely responsible for creating breakthroughs in terms of human performance that simply were not previously conceivable.[130] The benefits of the technology, however, are not without risk and raise emerging ethical questions.[131] The advancements in modern wearable technology provide greater insight into an athlete's private physiological information than ever available before.[132] There are numerous concerns around tracking athletes' physiological data, but the reliability of the information and its potential uses are likely at the forefront of these concerns for professional athletes.[133] While the NBA has prohibited the use of athlete tracking information in contract negotiations,[134] other leagues that have not fully developed policies in conjunction with players' associations could conceivably collect ABD for the express purpose of gaining advantages in negotiation. Similarly, without a negotiated right for athletes to access their data, it is not beyond the realm of possibility that team executives could misrepresent a players' fitness. We discuss the risks surrounding biometric data collection in depth in the following section.

IV. RISKS WITH THE USE OF BIOMETRIC DATA

The need to monitor the health of athletes goes beyond enhancing performance. It also serves to keep players healthy and avoid and monitor for injuries.[135] While the players themselves are valuable assets to a team, data about them is about to become a multi-billion-dollar industry.[136] Although many would desire as much data as possible about key players, there are a number of significant risks, to both the players and the teams, in the collection and the use of this data that this Article will address.

A. Privacy

The biggest risk to the monitoring of a player's biometric data is that the monitor will have access to a player's most personal habits, depending on what device is used and when. For example, many choose

130. *See* Jessop & Baker, *supra* note 37 (discussing former Florida State University football coach praising the insights derived from the football program's implementation of Catapult devices).

131. *See* James, *supra* note 119.

132. Katrina Karkazis & Jennifer R. Fishman, *Tracking U.S. Professional Athletes: The Ethics of Biometric Technologies*, 17 AM. J. BIOETHICS 45 (2016).

133. *Id.*

134. NBA–NBPA Collective Bargaining Agreement, *supra* note 105, at 361.

135. *See* John Patrick Pullen, *Why Professional Athletes Love This Fitness Band*, TIME (Apr. 18, 2017, 11:23 AM), https://time.com/4744459/whoop-strap-fitness-tracker-band/ [https://perma.cc/9ZQP-QWT7].

136. Glanz & Armendariz, *supra* note 12.

to wear their devices 24/7, which would reveal much more than athleticism. It can reveal a player's location at 3 a.m., as well as when they are engaging in sexual activity.[137] This data is only tangentially related to a player's health and performance and could needlessly be interpreted in a negative light. The law on the use of ABD in the U.S. is unclear.[138]

Privacy law in the U.S. is sectoral, meaning that the regulations address categories of information rather than personal data as a whole.[139] There is no overarching federal privacy statute, and unless the data is collected by a covered entity and is the category of data the regulation is meant to address, there is no statutory privacy protection for that data.[140] There are only a handful of states which have laws addressing biometric data, and the federal laws that would apply to ABD relate to data collected by medical professionals or employers.[141] Because ABD is collected by private third-party corporations, its protection is uncertain. Additionally, many athletes sign contracts

---

137. Andrew Boyd, *What Mapping Fitness and Sleep Data Can Reveal About Us*, NETWORKWORLD (June 15, 2015, 8:00 AM), https://www.networkworld.com/article/2934355/mapping-the-route-of-fitness-and-sleep-data-and-revealing-more.html. The information gathered can be quite revealing and invasive, even to unsophisticated observers. For example, a reporter for the NFL Network discovered that a former boyfriend was cheating on her because the synching of their FitBits allowed her to see that his physical activity levels were spiking at 4 a.m., when he was unaccounted for. *See* Jessica Guynn, *Fitbit Doesn't Fool Around: How the Fitness Tracker Helped this Woman Catch Her Boyfriend Cheating*, USA TODAY (Dec. 14, 2019, 10:00 AM), https://www.usatoday.com/story/tech/2019/12/14/fitbit-jane-slater-says-she-caught-ex-boyfriend-cheating-fitness-tracker/2642891001/ [https://perma.cc/PZ9L-4E4T].

138. Unlike the U.S., the EU has addressed privacy and data security issues with respect to biometric data in its General Data Protection Regulation (GDPR). General Data Protection Regulation 2016/679, 2016 O.J. (L 119) 1 [hereinafter GDPR]. In the EU, personal data is any information that is "relating to an identified or identifiable natural person," and biometric data and data concerning health are both considered a "special categories" of information subject to an increased level of protection under EU law. GDPR, at art. 4 & art. 9. The processing of special categories of information is generally prohibited in the EU unless an exception applies. This includes both physical and physiological data (e.g. heart rate) and behavioral data (e.g. lack of sleep the night before a game). The rule prohibits processing this data without explicit consent (or a recognized exception in the GDPR). The EU views consent differently than in the U.S. While the U.S. permits entities to collect data from its users unless a user opts out, the EU model requires users to opt in. W. Gregory Voss & Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*, 56 AM. BUS. L.J. 287, 339 (2019). When it comes to employer-employee situations, the EU has indicated doubt whether an employee can legally give their voluntary consent at all. In fact, the example of an athlete being asked to consent to video monitoring during practice by a sports club as being invalid consent is given in the Guidelines 3/2019 on processing of personal data through video devices. Guidelines 3/2019 on Processing of Personal Data Through Video Devices, European Data Protection Board 14 (Jan. 29, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf [https://perma.cc/VD2N-8F27].

139. *See* Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook? Or a New Paradigm in Data Privacy*, 25 RICHMOND J. L. & TECH. 1, 8 (2018) (discussing the limited protections provided by U.S. law for data privacy and security).

140. *Id.*

141. *See id.* at 19-25.

waiving their privacy rights regarding information about their health and performance.[142] There is an arguably lower expectation of privacy in an athlete's ABD than in the average citizen's biometric data.[143]

1. *Federal Law*

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, addresses the use of personal health information (which could include some biometric data).[144] HIPAA provides certain privacy protections for personal health information (PHI), including a prohibition on sharing the information without consent.[145] The reason this law most likely will not be interpreted to apply to ABD is because it is not collected by a "covered entity," but rather by the device maker itself.[146] The law only applies to covered entities, such as hospitals, physicians, group health plans, and medical billing companies.[147] It expressly does not apply to employers, state and local law enforcement, most state agencies, and schools.[148] Because ABD is generally collected by an employer or private third-party company, HIPAA's application is unlikely.[149] Additionally, HIPAA specifically excludes mobile health

---

142. *See generally,* James Blake Hike, *An Athlete's Right to Privacy Regarding Sport-Related Injuries: HIPAA and the Creation of the Mysterious Injury,* 6 IND. HEALTH L. REV. 47, 72-74 (2009) (describing the role of waivers and disclosure of health information).

143. *See, e.g.*, Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 657 (1995) (noting that athletes in a school setting have a reduced expectation of privacy because of the shared nature of locker rooms).

144. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191; 45 C.F.R. §164.514 (b)(2)(i)(P).

145. Final Omnibus HIPAA Rule Preamble, 78 Fed. Reg. 5568-01, 5572 (1996).

146. *See* 45 C.F.R. § 160.103 (1996) (describing the law's application).

147. *Id.*

148. *See Health Privacy: HIPAA Basics,* PRIVACY RIGHTS CLEARINGHOUSE (Feb. 1, 2015), https://privacyrights.org/consumer-guides/health-privacy-hipaa-basics#:~:text=HIPAA%20does%20not%20protect%20all,entities%20and%20their%20business%20associates [https://perma.cc/EL3C-XPSD] (describing who is an who is not a "covered entity" under HIPAA).

149. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, at 52 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/533U-FLHW] (noting that frequently "health apps are collecting [private patient information, such as their medical history,] through consumer-facing products, to which HIPAA protections do not apply"); Jillisa Bronfman, *Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population,* 14 DUKE L. & TECH. REV. 192, 201-02 (2016) (contending that "if the entity gathering health data is not a covered provider like a hospital or medical care provider, there is no protection from HIPAA"); Elizabeth A. Brown, *The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work,* 16 YALE J. HEALTH POL'Y L. & ETHICS 1, 24 (2016) ("When a Fitbit or iPhone app tells an employer how much an employee has exercised, what her heart rate is, or how high her blood sugar levels are, those data do not fall within the scope of HIPAA protection."); Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things,* 59 B.C. L. REV. 423, 497 n.381 (2018) (citing Elizabeth Snell, *How Do HIPAA Regulations Apply to Wearable Devices?,* HEALTH IT SEC. (Mar. 23, 2017),

devices and wearables known as "mHealth technologies" from its protection, leaving federal regulation to the Federal Trade Commission (FTC), Food and Drug Administration (FDA), and Federal Communications Commission (FCC).[150] Regardless of what information is included, the businesses collecting and processing data from mHealth technologies are considered non-covered entities under HIPAA.[151] The FTC is in charge of protecting consumers from "unfair or deceptive acts or practices in or affecting commerce" under Section 5 of the FTC Act, which includes violating the terms of a company's privacy promises.[152] The FTC has issued guidance on the use of biometric information.[153] The FCC has established the Connect2HealthFCC task force to create a set of regulations addressing health technology.[154] The FDA has also created nonbinding guidance on medical mobile apps.[155]

Although HIPAA does not generally cover ABD, some of the data could be regulated under HIPAA if a covered entity collects it, such as a medical professional; however, a team doctor would probably be excluded as an agent of the employer.[156] Additionally, the purpose of the data's collection would have to be for health care purposes, as opposed

---

http://healthitsecurity.com/news/how-do-hipaa-regulationsapply-to-wearable-devices ("[W]here a company that offers a wearable, or a mobile app that collects health information, where that arrangement is just directly between the device maker and the individual. Or it's between the app maker and the individual, and there's no covered entity or business associate involved. Then there's no application of HIPAA . . . .") (internal quotation marks omitted)).

150. Elvy, *supra* note 149; *Mobile Health Apps Interactive Tool*, FED. TRADE COMM'N (Apr. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool [https://perma.cc/BE28-YFBJ]; Steven Tucker, *Welcome to the World of mHealth!*, 1 MHEALTH 1 (2015).

151. *See* Elizabeth Snell, *How Do HIPAA Regulations Apply to Wearable Devices?*, HEALTH IT SEC. (Mar. 23, 2017), https://healthitsecurity.com/news/how-do-hipaa-regulations-apply-to-wearable-devices [https://perma.cc/8JNA-34CR] ("There is a lot of ambiguity about exactly where HIPAA is triggered and where it's not. . . . The only real clarity is where a company that offers a wearable, or a mobile app that collects health information, where that arrangement is just directly between the device maker and the individual. Or it's between the app maker and the individual, and there's no covered entity or business associate involved. Then there's no application of HIPAA, that's clear.")

152. 15 U.S.C. § 45(a)(1) (2006); *See Mobile Health App Developers: FTC Best Practices*, FED. TRADE COMM'N (Apr. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices#other [https://perma.cc/R4TK-ALAA] (providing tailored advice to health app developers).

153. *Id.*

154. *Connect2HealthFCC*, FED. COMMC'NS COMM'N, https://www.fcc.gov/about-fcc/fcc-initiatives/connect2healthfcc [https://perma.cc/W6YQ-VWDV].

155. The FTC's Mobile Device Apps Interactive Tool provides a series of questions for an app developer to answer to determine which laws apply to it. *See Mobile Health Apps Interactive Tool*, FED. TRADE COMM'N (Apr. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool [https://perma.cc/V9UE-LQVA].

156. *See What Federal Laws Apply to Biometrics*, ELEC. FRONTIER FOUND., https://www.eff.org/sls/tech/biometrics/faq#faq-What-federal-laws-apply-to-biometrics? [https://perma.cc/Y9RW-YDW6].

to performance.[157] A report issued pursuant to Section 13424 of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009 suggests how Congress can fill the large gaps in HIPAA due to mobile health technologies.[158]

With respect to student athletes, the Family Educational Rights and Privacy Act (FERPA) could provide some protection.[159] Universities that receive funds from the U.S. Department of Education may not share personally identifiable information (PII) about students without their consent.[160] The definition of PII in § 99.3 of the statute includes biometric data.[161] However, student athletes likely do consent to the use of this data in exchange for the ability to play on the team and/or scholarship.[162]

Although there is no overarching federal law regarding biometric data protection, a handful of states have addressed this issue.[163]

2. *State Biometric Laws*

Currently, only three states have taken up the issue of biometric data, and their protections all originate from a privacy perspective.[164] Illinois was the first state to enact a privacy law regarding biometric technology.[165] It not only requires consent to collect the data; it also

---

157. Osborne & Cunningham, *supra* note 35, at 47-57 (discussing the limitation of HIPAA to the different types of data collected by sports teams).

158. *See* U.S. DEP'T OF HEALTH AND HUMAN SERVICES, EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA, at 1-6 (July 19, 2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf [https://perma.cc/8J35-V44R].

159. 20 U.S.C. § 1232g(c); 34 C.F.R. Part 99 (2013).

160. 34 C.F.R. § Part 99.30 (2013).

161. *Id.*; *See also* Brian H. Lam, *Athletes and Their Biometric Data – Who Owns It and How It Can Be Used*, NAT'L L. REV. (Dec. 19, 2017), https://www.natlawreview.com/article/athletes-and-their-biometric-data-who-owns-it-and-how-it-can-be-used [https://perma.cc/WM7R-FBPN].

162. *See generally* 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 (2017).

163. *See, e.g.*, 740 ILL. COMP. STAT. ANN. 14/15 (West 2008); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017); WASH. REV. CODE ANN. § 19.375.010 (West 2017).

164. 740 ILL. COMP. STAT. ANN. 14/15 (West 2008); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017); WASH. REV. CODE ANN. § 19.375.010 (West 2017). However, several other states have added biometric data to their definition of personal data in their data breach statutes. *See* WIS. STAT. ANN. § 134.98 (West 2007); ARK. CODE. ANN. § 4-110-103(7)(c) (West 2019) (revising the Arkansas Code to include biometric data in the definition of "personal information"); Stop Hacks and Improve Electronic Security Act, N.Y. GEN. BUS. LAW § 899-aa (West 2019) (amended through the SHIELD Act); COLO. REV. STAT. §§ 6-1-713(2)(b), 6-1-713.5 (2018); MD. CODE ANN., COM. LAW § 14-3501(e)(1) (West 2018); 2021 VA. ACTS Chpt. 36 (passed as the Virginia Consumer Data Protection Act, effective January 1, 2023).

165. The biometric data covered by the Illinois statute at 14/10 ("biometric identifier") is limited to "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" and

limits what may be collected, how the data is to be secured, and how long it can be retained.[166] It strictly regulates how private parties may use biometric data. Importantly, the Biometric Information Privacy Act (BIPA) "prohibits private entities from selling biometric information, restricts the disclosure thereof, and requires reasonable care be taken in storing or transmitting biometric identifiers/information."[167] Although BIPA does not specifically address ownership of biometric data, it does provide very detailed and significant privacy protections to those from whom data is collected.[168] Similar to European law, it relies on a system of disclosure and consent.[169] Related to ownership, however, is the prohibition on selling, leasing, trading, or otherwise profiting from that biometric information.[170] One of the unique features of BIPA is the private right of action given to individuals whose biometric data has been used contrary to the statute.[171]

The Texas Biometric Privacy Act does not require consent to collect biometric data, but does require consent for selling or leasing the data.[172] Similar to BIPA, it contains data protection requirements and a data retention provision of one year.[173] Washington's biometric law expressly excludes "physical or digital photograph, video or audio

---

"any information regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." As such, it would only apply to specific categories of ABD. 740 ILL. COMP. STAT. ANN. 14/10 (West 2008); *see* 740 ILL. COMP. STAT. ANN. 14/15 (West 2008).

166. BIPA section 14/15(b) provides that biometric data cannot be collected unless written informed consent is obtained. Section 14/15 (a) and (e) indicate that biometric data must be given the same security protections provided to confidential information and outlines clear policies regarding retention and storage. 740 ILL. COMP. STAT. ANN. 14/15 (West 2008).

167. 740 ILL. COMP. STAT. ANN. § 14/15(c)-(d) (West 2008). *See* P. Russell Perdew et al., *Second Circuit Delivers Limited Victory to Defendant Under Illinois Biometric Privacy Act and Spokeo*, LOCKE LORD (Nov. 22, 2017), https://www.lockelord.com/newsandevents/publications/2017/11/bipa-and-spokeo [https://perma.cc/RKT3-ZTPN].

168. 740 ILL. COMP. STAT. ANN. 14/15(c)-(d) (West 2008).

169. *See infra* Part VI.

170. 740 ILL. COMP. STAT. ANN. 14/15 (West 2008).

171. The Illinois Supreme Court reversed the lower court and found that individuals could sue despite not showing economic harm because their "right to control" their information was violated. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1206 (Ill. 2019). This is contrary to how most federal courts have interpreted "harm" under privacy statutes denying claims for what they label "technical violations" of the statutes. *See generally* Anna L. Metzger, *The Litigation Rollercoaster of BIPA: A Comment on the Protection of Individuals from Violations of Biometric Information Privacy*, 50 LOYOLA U. CHI. L.J. 1051 (2019), https://www.luc.edu/media/lucedu/law/students/publications/llj/pdfs/vol50/issue-4/18_Metzger%20(1051-1100).pdf [https://perma.cc/745K-5ZP5]; *see also Data Protection Law: An Overview*, CONG. RES. SERV. 59-62 (Mar. 2019), https://sgp.fas.org/crs/misc/R45631.pdf [https://perma.cc/C7SL-P2H2] (regarding the necessity of harm for standing under federal privacy law).

172. The biometric data covered by the Texas statute ("biometric identifier") is limited to "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry." As such, it would only apply to specific categories of ABD. TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).

173. *Id.*

recording or data generated therefrom" but it does include "unique biological patterns or characteristics that [are] used to identify a specific individual," which may apply to athletic biometric information.[174] Although BIPA provides a private right of action for individuals whose data is used in violation of the law, in Texas and Washington, only the attorney general can enforce their biometric data statutes.[175]

California does not have a law specific to biometric data; however, the California Consumer Privacy Act (CCPA), which became effective January 1, 2020, does include biometric data.[176] The CCPA definition of biometric data includes "an individual's physiological, biological or behavioral characteristics, including an individual's . . . (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity."[177] There are several rights given to California consumers to protect their personal information and biometric data that include:

- Accessing the data (right of disclosure or access);[178]
- Deleting the data (right to be forgotten);[179]
- Transferring the data (data portability—the data must be received in a commonly used and readable format);[180]
- Requesting businesses not to sell their personal information;[181]
- Opting out of the collection or sharing of the data (Opt-in is the primary consent standard mandated by European GDPR);[182] and,
- Right of action (penalties).[183]

---

174. The biometric data covered by the Washington statute ("biometric identifier") is limited to "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual." As such, it would only apply to specific categories of ABD. WASH. REV. CODE ANN. § 19.375.010 (West 2017).

175. Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107, 118 (Mar. 25, 2019). Additionally, several other states are considering biometric data protection legislation, including Arizona, Florida, and Massachusetts. Molly McGinley & Kenn Brotman, *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, NAT'L L. REV. (Mar. 25, 2019), https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states [https://perma.cc/YC7L-YGBU].

176. CAL. CIV. CODE § 1798.140 (West 2020) (passed as the California Consumer Privacy Act).

177. CAL. CIV. CODE § 1798.140(b) (West 2020).

178. CAL. CIV. CODE § 1798.100 (West 2020).

179. CAL. CIV. CODE § 1798.105 (West 2020).

180. CAL. CIV. CODE § 1798.100(d) (West 2020).

181. CAL. CIV. CODE § 1798.120 (West 2020).

182. *Id.*

183. CAL. CIV. CODE § 1798.150-55 (West 2020); Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, PRAC. L. (2018), https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf [https://perma.cc/PW3K-L5AD].

These statutes provide some protections to consumers with respect to their data, although they are primarily notice and consent statutes—meaning that consumers can consent to the sharing, leasing, and sale of their biometric data by the company collecting the data.[184] BIPA has stronger protections than Texas and Washington and would require more stringent notifications and consent provisions before being able to monetize the data.[185]

B. Employment Law

In addition to privacy issues, athletes may be concerned about how the data could be used against them. For example, ABD could be used in contract negotiations, to punish an athlete who is not following exercise protocol, or even subpoenaed in a criminal trial to demonstrate proximity to a crime.[186] Several athletes have had adverse employment

---

184. Concerning the sale, lease, and disclosure of biometric identifiers, the Washington statute permits these activities if "consent has been obtained from the individual." Wash. Rev. Code § 19.375.020(3) (2017); Allison Grande, *Wash. Expands Biometric Privacy Quilt with More Limited Law*, LAW360 (July 21, 2017, 7:15 PM), https://www.law360.com/articles/934030/print?section=consumerprotection [https://perma.cc/9A9F-AY5P] (contending that "Washington deviates sharply from Illinois by omitting hotly contested provisions that businesses argue expose them to heightened legal liability, notably the right of consumers to sue and for companies to be held accountable for the collection and handling of digital photographs and audio recordings").

185. TEX. BUS. & COM. CODE ANN. § 503.001(b)-(c) (West 2017) ("(c) A person who possesses a biometric identifier of an individual that is captured for a commercial purpose: (1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless: . . . [(c)(1)](C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code . . . ."); 740 ILL. COMP. STAT. ANN. 14/15(d) (West 2008) ("No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless: . . . (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance . . . ."); Elvy, *supra* note 149, at 494 (citing WASH. REV. CODE ANN. § 19.375.020(3) (West 2017) ("Unless consent has been obtained from the individual, a person who has enrolled an individual's biometric identifier may not sell, lease, or otherwise disclose the biometric identifier to another person for a commercial purpose unless the disclosure: . . . (d) [i]s required or expressly authorized by a federal or state statute, or court order . . . .")).

186. Recently a man using an exercise tracking device while riding his bike was notified by Google that the police had requested his data in connection with a burglary, simply due to his proximity to the crime scene. Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect*, NBC NEWS (Mar. 7, 2020, 6:22 AM), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/P9MB-YGVY] ("The app [RunKeeper] relied on his phone's location services, which fed his movements to Google. He looked up his route on the day of the March 29, 2019, burglary and saw that he had passed the victim's house three times within an hour, part of his frequent loops through his neighborhood, he said. . . . Google geofence warrants have been used by police agencies around the country, including the FBI. Google said in a court filing last year that the requests from state and federal law enforcement authorities were increasing rapidly: by more than 1,500 percent from 2017 to 2018, and by 500 percent from 2018 to 2019."). As a result of a relative's act of providing DNA to GEDmatch, a website that helps people track their ancestry, the Golden Gate Killer was identified. While some applauded this novel use, others were horrified that law enforcement

actions taken against them due to biometric screening.[187] For example, NBA player Eddy Curry's contract was not renewed with the Chicago Bulls after a genetic test revealed that he had a heart condition.[188]

ABD presents a unique employment law issue because (1) there is no federal law protecting the privacy and use of biometric data, and (2) athletes generally consent to the monitoring of their ABD, which could be interpreted as waiving their rights under employment law.[189] A few cases regarding the use of health data in employment situations may be instructive, but the sectoral nature of the laws and the lack of updates to the laws based on new technologies make it difficult to apply those cases to current situations.[190] Because of the high cost of employee healthcare coverage in the United States, employers look for ways to keep costs down with high deductible plans and workplace health programs.[191] As a result, employers have begun to track employees' health through wearables.[192] Because this information is not collected by "covered entities" under HIPAA, it is not subject to protection as PHI.[193] The way employers get employees to allow this monitoring is by offering incentives such as reduced insurance premiums, a

---

could so easily access DNA and use analytics to identify someone who had committed a crime. Certainly, when this relative added their biometric data to the website, he or she had no indication that their data would go beyond tracking down lost relatives. GEDmatch has since changed its policy to require explicit consent for this type of data use. Andrea Marks, *DNA Search Method that Caught Golden State Killer No Longer Available*, ROLLING STONE (May 23, 2019, 5:21 PM), https://www.rollingstone.com/culture/culture-news/dna-search-method-that-caught-the-golden-state-killer-no-longer-available-839315/ [https://perma.cc/B3MU-UU5X].

187. Roberts, *supra* note 56. *Cf.* NBA–NBPA Collective Bargaining Agreement, *supra* note 105, at 381 (Sec. 13(h): "The data may not be considered, used, discussed or referenced for any other purpose such as in negotiations regarding a future Player Contract or other Player Contract transaction (*e.g.*, a trade or waiver) involving the player.").

188. A.E. Rice, *Eddy Curry and the Case for Genetic Privacy in Professional Sports*, 6 VA. SPORTS & ENT. L.J. 1 (2006).

189. *See* Osborne & Cunningham, *supra* note 35, at 53.

190. For a discussion of the enormous gaps in PHI protection with respect to collection by commercial entities, see Janine S. Hiller, *Healthy Predictions? Questions for Data Analytics in Health Care*, 53 AM. BUS. L.J. 251, 301 n.282 (2016).

191. Stephen Miller, *15 Ways Employers Can Reduce Health Care Spending That Aren't Cost-Sharing*, SHRM (Feb. 27, 2019), https://www.shrm.org/resourcesandtools/hr-topics/benefits/pages/top-ways-employers-hold-down-healthcare-spending.aspx [https://perma.cc/8P3R-UFXL].

192. *See generally* David Cox, *The Rise of Employee Health Tracking*, BBC (Nov. 10, 2020), https://www.bbc.com/worklife/article/20201110-the-rise-of-employee-health-tracking [https://perma.cc/6DBX-345G] (describing an increase of employers tracking employees' health information).

193. *See* Risa Boerner, *Employers Considering the Use of Wearables To Combat COVID-19 Need to Anticipate Privacy Considerations*, JD SUPRA (June 2, 2020), https://www.jdsupra.com/legalnews/employers-considering-the-use-of-37699/ [https://perma.cc/T4AL-999K] (noting that employers will largely not be subjected to HIPAA restrictions because they are not, generally, "covered entities").

deductible credit, or through free devices.[194] In 2018, twenty percent of employers who offered health insurance were collecting health data from wearables.[195] Many employees do not fully realize how their data is shared. It is not solely for their benefit. The data may be viewed by their employers, their health insurance company, and the manufacturer of the device who may then sell that information due to the lack of omnibus privacy law in the U.S.[196] Additionally, fifty percent of large employers offer biometric health screening, with fifteen percent rewarding or penalizing employees for the screening outcome.[197] The employees' willingness to sign on to these programs stems from the misguided belief that all health data is subject to HIPAA.[198]

The main statute applicable to using health information to discriminate is the Americans with Disabilities Act (ADA).[199] This federal law prevents covered employers from discriminating against qualified individuals with disabilities regarding "job application procedures, the hiring, advancement, or discharge of employees, employee compensation, job training, and other terms, conditions, and privileges of employment."[200] A disability is a physical or mental impairment that substantially limits a major life activity.[201] In an article by Professor Jessica Roberts and others titled: *Evaluating Player Health and Performance: Legal and Ethical Issues*, the authors make the argument that most NFL practices, such as medical examinations at the Combine and as a condition of employment, violate the ADA.[202] Because the National Football Scouting corporation runs the Combine, it may not be considered an employer for ADA purposes unless it is considered an agent of the NFL.[203] The authors also point out the uncertain status of biometric data collected during the Combine that could reveal

194. UnitedHealthcare Motion, for example, will give employees enrolled in the program up to $1,000 a year if they hit certain step goals (such as the common 10,000 steps a day goal). Christopher Rowland, *With Fitness Trackers in the Workplace, Bosses Can Monitor Your Every Step — and Possibly More*, WASH. POST (Feb. 16, 2019), https://www.washingtonpost.com/business/economy/with-fitness-trackers-in-the-workplace-bosses-can-monitor-your-every-step--and-possibly-more/2019/02/15/75ee0848-2a45-11e9-b011-d8500644dc98_story.html [https://perma.cc/8XAS-G7J9].

195. *Id.*

196. *Id.*

197. *2018 Employer Health Benefits Survey*, KAISER FAM. FOUND. (Oct. 3, 2018), https://www.kff.org/report-section/2018-employer-health-benefits-survey-summary-of-findings/ [https://perma.cc/WA9Y-3Y9M].

198. *See* Boerner, *supra* note 193 (noting that HIPAA only applies to covered entities).

199. Americans with Disabilities Act, 42 U.S.C. §§ 12101-12213 (2018).

200. 42 U.S.C. § 12112(a).

201. 42 U.S.C. § 12102(1).

202. Jessica L. Roberts et al., *Evaluating NFL Player Health and Performance: Legal and Ethical Issues*, 165 U. PA. L. REV. 227, 227 (2017).

203. *Id.* at 305.

an impairment.[204] The authors make the analogy of the physical fitness tests required of firefighters as not being "medical examinations" and thus not violative of the ADA.[205]

The law also protects employees against discrimination when the employee is regarded as having "such an impairment."[206] While an employee may not be a "qualified individual" if their disability would prevent them from engaging in the sport for which they are hired, it is the second prong that presents a novel legal issue.[207] If biometric data indicates an athlete has an arm impairment, but the employee believes they are otherwise qualified (meaning they can engage in the sport for which they were hired), are they protected under the ADA?[208] If an employee has permanent damage to her leg and can no longer play soccer, she would not receive protection. If, however, she has recovered from an injury and is ready to play, and her performance specs indicate that she is playing at the level she did before the injury, but a report analyzing her biometric data indicates that she is still in recovery and as a result is benched, or worse yet, released from the team, would she have a claim for discrimination? The report would seemingly fall under the category of being regarded as having an impairment, but her performance indicates that she is qualified.[209]

The seminal case involving the ADA in professional sports is *PGA Tour, Inc. v. Martin*, where a professional golfer challenged the "no cart" rule of the PGA due to an impairment affecting his ability to walk.[210] Because the golf cart was deemed to be a "public accommodation" under Title III of the ADA, the tournament was required to

---

204. *Id.*

205. *Id.* at 306.

206. 42 U.S.C. § 12102(1)(C).

207. Eric Bachman, *ADA "Perceived as Disabled" Employment Lawsuits in the Age of Covid-19*, FORBES (Aug. 20, 2020, 10:12 AM), https://www.forbes.com/sites/ericbachman/2020/08/20/ada-perceived-as-disabled-employment-lawsuits-in-the-age-of-covid-19/?sh=2f67009c3150 [https://perma.cc/A9A4-GZKH].

208. Consider, for example, the case of NBA player Reggie Lewis, who continued playing basketball after being diagnosed with a heart condition and told to discontinue playing, choosing to rely instead on a second opinion that informed him that he did not have a serious heart condition. *See* Robert M. Thomas, Jr., *Pro Basketball; Celtics' Lewis Dies After Collapsing in a Gym*, N.Y. TIMES (July 28, 1993), https://www.nytimes.com/1993/07/28/sports/pro-basketball-celtics-lewis-dies-after-collapsing-in-a-gym.html [https://perma.cc/4CWF-RHJ5].

209. The ADA is also applicable to college athletes. While the ADA applies to private entities and places of public accommodation, the Rehabilitation Act of 1973 applies to recipients of federal funds, which generally include colleges and universities. 29 U.S.C. § 794(a) (2018). For a detailed explanation on how the ADA applies to student athletes, see Yuri Nicholas Walker, *Playing the Game of Academic Integrity vs. Athletic Success: The Americans with Disabilities Act (ADA) and Intercollegiate Student-Athletes with Learning Disabilities*, 15 MARQ. SPORTS L. REV. 601 (2005); Maureen A. Weston, *Academic Standards or Discriminatory Hoops? Learning-Disabled Student Athletes and the NCAA Initial Academic Eligibility Requirements*, 66 TENN. L. REV. 1049, 1066 (1999); *see also* 34 C.F.R. § 104.47.

210. 532 U.S. 661 (2001).

provide this "reasonable accommodation."[211] It should be noted that this was a public accommodation case, not an employment discrimination case, but it is instructive in establishing that the ADA could apply to professional athletes.[212]

The Genetic Information Nondiscrimination Act (GINA) prohibits discrimination based on genetic information, which includes data collected with a blood test and family medical history information.[213] Although courts have not resolved these issues around ABD, according to Professors Karkazis and Fishman, authors of *Tracking U.S. Professional Athletes: The Ethics of Biometric Technologies*, the ability for athletes to claim protection under the ADA or GINA is very unlikely.[214] Although the ADA is intended to prevent employers from discriminating on the basis of a disability, it does allow an employer to argue that the athlete is not a "qualified individual."[215] With respect to GINA, the law does contain an exception to coverage for "wellness programs," of which wearables are arguably a component.[216]

C. *Erroneous Data*

There is also a concern regarding the collection and use of biometric data, aside from privacy and employment risks, that it may not actually reflect what it purports to indicate. Erroneous data or data which is wrongly interpreted could have far-reaching implications for an athlete's scholarship or career. If the data is not accurate, this can present problems that would not exist without the device. There is a tendency to believe that data is infallible.[217] However, there are numerous

---

211. Michael Cottingham et al., *The Historical Realization of the Americans with Disabilities Act on Athletes with Disabilities*, 26 J. LEGAL ASPECTS SPORT 5 (2016).

212. *PGA Tour, Inc.*, 532 U.S. at 690-91.

213. Had GINA been in effect at the time, Eddy Curry would have likely had a claim of genetic discrimination. Roberts, *supra* note 56, at 66.

214. Karkazis & Fishman, *supra* note 132, at 55.

215. Jonathan R. Cook, *The Americans with Disabilities Act and Its Application to High School, Collegiate and Professional Athletics*, 6 JEFFREY S. MOORAD SPORTS L.J. 243, 246-47 (1999) ("If the athlete proves he is qualified and suffered discrimination because of his disability, the burden shifts to the athletic association to prove that: (1) the eligibility requirements are essential and neutral on their face and as applied; and (2) the only accommodation that would enable the athlete to participate in a sport requires a waiver of the eligibility requirements that would fundamentally alter the nature of the program.") (citation omitted).

216. Lisa McGlynn, *Checking in on GINA: Revisiting the EEOC's Rules on the Genetic Information Nondiscrimination Act*, FISHER PHILLIPS (Nov. 3, 2017), https://www.fisherphillips.com/Employment-Privacy-Blog/checking-in-on-gina-revisiting-the-eeocs#:~:text=However%2C%20GINA%20provides%20an%20exception,care%20professional%20or%20counselor%20receive [https://perma.cc/Y7GQ-RL66].

217. *See* Lloyd Hitoshi Mayer, *The Promises and Perils of Using Big Data to Regulate Nonprofits*, 94 WASH. L. REV. 1281, 1310 (2019); *see also* Danah Boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, 15 INFO. COMMC'N & SOC'Y 662, 666 (2012).

examples of mistakes that can result in inaccurate outputs.[218] For example, research demonstrates that common methods of heart rate monitoring do not accurately assess athlete wellness and fatigue.[219]

Additionally, commercial products that use detailed health and social data, analytics, and algorithms to create predictive models for patient care and health operation efficiencies have been dubbed "black boxes" due to "the use of opaque computational models to make decisions related to health care."[220] As predictive analytics are incorporated into biometric data analysis, their accuracy becomes important if a player's athletic "life" can be predicted. For example, predictive analytics could predict how long a player's knees will hold out, potentially resulting in a release from the team based on the output of a computer program. If there is no guarantee that the prediction is accurate, decisions can be made based on flawed science.[221]

There are numerous steps in the process where mistakes can be made: players' incorrect use of the device; mechanical malfunction of the device; incorrect coding or categorization of data; and use of a faulty algorithm.[222] Making multi-million-dollar decisions based on algorithmic outputs can have significant effects on players, their teams, their families, and their fans.[223]

D. Data and Security Breaches

Additionally, there is the risk of harm resulting from insufficient care in protecting the data from accidental disclosure due to lax security measures or keeping it protected from hackers. Like financial information, this data could be very attractive to a certain segment of

---

218. *See, e.g.*, Christopher Schneider, *Heart Rate Monitoring in Team Sports—A Conceptual Framework for Contextualizing Heart Rate Measures for Training and Recovery Prescription*, 9 FRONTIERS PHYSIOLOGY 639 (2018), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5990631/ [https://perma.cc/JC8P-MEVX].

219. *Id.*

220. Hiller, *supra* note 190, n.282 (citing W. Nicholson Price II, *Black-Box Medicine*, 28 HARV. J.L. & TECH. 419, 421 (2015)).

221. Lidong Wang & Cheryl Ann Alexander, *Big Data Analytics in Biometrics and Healthcare*, 6 J. COMPUTER SCI. & APPLICATIONS 48 (2018) (explaining the privacy and security challenges of biometrics in biometric data analytics).

222. For a discussion on issues with medical analytics, see Sharona Hoffman, *Big Data Analytics: What Can Go Wrong*, 15 IND. HEALTH L. REV. 227, 227, 246 (2018) (outlining areas where mistakes can occur such as in "data quality deficiencies; selection, confounding, measurement, and confirmation biases; inadequate sample sizes; sampling errors; effect modifiers; and causal interactions . . . . All of these can cause researchers to mistake mere associations for causal relationships and to reach conclusions that are invalid and cannot be replicated in subsequent studies. Erroneous research findings can mislead legislators, regulators, and lawyers who use them for purposes of policy-making or litigation. . . . [T]he pitfalls of big data analysis are numerous, and anyone conducting, reviewing, or relying upon it must be aware of their existence").

223. Karkazis & Fishman, *supra* note 132 (suggesting that data measurements should be verified as being more accurate than current methods and outlining the ethical considerations with the use of ABD).

the population, such as opposing teams and those who make wagers on sports teams. Without adequate security protections for this data, it could easily be made available to parties with ill intent.[224] In one highly publicized case, the scouting director for the St. Louis Cardinals was sentenced to four years in prison for hacking into the Houston Astros database.[225]

Many scholars have brought attention to the cybersecurity risks that the Internet of Things ("IoTs") presents.[226] The value of the databases held by teams, regarding their players, cannot be overstated. Rival teams, those who place sporting bets, and fantasy league players would all desire access to any morsel of information about a player—especially if the information is not publicly known; thus, creating an incentive to engage in cyber espionage for the purpose of gaining access to these databases.[227] In addition to the databases, there is the added issue of the security of the devices themselves.[228] Opposing teams could gain information about a player based on the player's activity the night before a big game.[229] Most concernedly, "cybersecurity threats may endanger the integrity of a league's games i[n] the emerging sports gambling marketplace."[230]

---

224. *See* Ifeoma Ajunwa, *Workplace Wellness Programs Could Be Putting Your Health Data at Risk*, HARV. BUS. REV. (Jan. 19, 2017), https://hbr.org/2017/01/workplace-wellness-programs-could-be-putting-your-health-data-at-risk [https://perma.cc/7B3J-2QCR].

225. *Christopher Correa, Former Cardinals Executive, Sentenced to Four Years for Hacking Astros' Database*, N.Y. TIMES (July 18, 2016), https://www.nytimes.com/2016/07/19/sports/baseball/christopher-correa-a-former-cardinals-executive-sentenced-to-four-years-for-hacking-astros-database.html [https://perma.cc/N6MF-QSJM].

226. Nathanial Grow & Scott J. Shackelford, *The Sport of Cybersecurity: How Professional Sports Leagues Can Better Protect the Competitive Integrity of Their Games*, 61 B.C. L. REV. 473 (describing that while teams have been quick to adopt wearables, they have been slow to adopt measures to prevent manipulation of these technologies).

227. *Id.* at 28. The Cardinals hacking scandal occurred when Carlos Correa, a Cardinals employee, gained access to the Houston Astros databases by using the modified versions of passwords of Astros employees who had formerly been St. Louis Cardinals' employees. *See* Ben Reiter, *What Happened to the Houston Astros' Hacker*, SPORTS ILLUSTRATED (Oct. 4, 2018), https://www.si.com/mlb/2018/10/04/chris-correa-houston-astros-hacker-former-cardinals-scouting-director-exclusive-interview [https://perma.cc/NMH8-5T5M].

228. In February 2020, hackers obtained data on two million Fitbit users, including location, sleep, health, and fitness information. *2 Million Fitbit Accounts Were Exposed by Cybercriminals*, HACKERNOON (Feb. 11, 2020), https://hackernoon.com/2-million-fitbit-accounts-was-exposed-by-cybercriminals-aa7u36pj [https://perma.cc/TKF8-LXM3].

229. An athlete's biometric status impermissibly obtained by someone looking to participate in a betting market would provide a distinct advantage to that individual, as they would possess otherwise unavailable information. *See* James, *supra* note 119. Standardized injury reporting is one of the measures that many sports leagues (though not all) have taken to reduce the value of insider information. *See* John T. Holden, *Why Are There No NCAA Injury Reports in the Age of Legal Sports Betting?*, LEGAL SPORTS REP. (Apr. 15, 2019), https://www.legalsportsreport.com/31209/ncaa-injury-reports-legal-sports-betting/ [https://perma.cc/JX5K-4ZM6].

230. Grow & Shackelford, *supra* note 226, at 497.

V. BIOMETRIC DATA OWNERSHIP

The few federal laws that do provide privacy protection do not clearly address the ownership of the subject data.[231] The ubiquitous nature of devices with sensors collecting massive amounts of data and concerns over data breaches and privacy have overshadowed another area—that of data ownership. Whoever owns the data not only controls it but can also monetize it. Biometric data ownership is a relatively new concept.[232] Intellectual property law was written long before the development of much of the technology used today, and courts have been inconsistent with their application on ownership of derived data.[233] One of the issues with biometric data ownership is that there are multiple parties involved in its creation: the individual from whom the data was collected; the team or union who may have requested the data to be collected or provided the individual with the device to track the data; and the creator of the device. Contract law is of limited use because all three sides have differing levels of involvement and conflicting desires for the use of the information. After discussing how data can be defined, this Part will explain the limitations of current law.

A. Legal Issues with defining ABD

ABD can be divided into "raw" and "derived" data. Raw data is the data directly collected from a player wearing a device, such as her heart rate. Derived data is created from data analytics. For example, a device tracking a player's speed over time can issue a report predicting a physical condition based on a decrease in speed over time. Because U.S. law does not address this distinction, the law of the EU may be instructive. Although the EU's use restrictions are more advanced than in the U.S., neither jurisdiction has fully addressed the ownership issue.

1. Biometric "Raw" Data

Although, in theory, individuals in the U.S. could own data collected about them, this is not the current model. By using websites and apps,

---

231. *See* Determann, *supra* note 59, at 22 (privacy laws in the U.S. are intended to protect individual freedom and dignity, not to allocate ownership of the data they protect).

232. Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 N. KY. L. REV. 29, 62 (2016) (discussing the lack of clarity regarding whether consumers or merchants own IoT data and contending that "the consumer owns the physical media where the data is stored," but different merchants "along the data processing chain can assert valid ownership of such data").

233. Determann, *supra* note 59, at 11 n.54 ("Patent law excludes laws of nature, natural phenomena, and abstract ideas from patentable subject matter. Trademark law denies protection for generic marks. Copyright law excludes facts and ideas from copyright protection.") (citing Mayo Collaborative Servs. v. Prometheus Lab'ys, Inc., 566 U.S. 66, 70-71 (2012); Park 'n Fly v. Dollar Park & Fly, 469 U.S. 189, 194 (1985); 17 U.S.C. § 102(b) (2012)).

most individuals are allowing companies to collect, use, and sell their data in exchange for access to the website or app without monetary compensation. Additionally, these companies' ability to collect, use, and sell data occurs with little statutory oversight and is generally permitted via a Terms of Use and is thus governed by contract law.[234] As discussed later in greater depth, facts and information cannot be owned under copyright law in the U.S.[235] The legal concept of "ownership" in the U.S. is usually described as a "bundle of sticks," which may be kept, loaned, given away, subordinated, or sold as the owner sees fit.[236] This model does not translate to data ownership, as data is regularly collected surreptitiously through websites that can keep, loan, give away, subordinate, or sell it as they see fit.[237] However, neither the individual from which the data is collected nor the company collecting it is considered the "owner" under that term's historical understanding.[238]

As mentioned above, in the U.S., individuals do not own their health information.[239] Although HIPAA provides the right for patients to "inspect, have a copy of and propose amendments" to their PHI, it is the medical practice that possesses the data.[240] In fact, under HIPAA,

---

234. *See, e.g.*, Gretchen Frazee, *Google Bought Fitbit. What Does That Mean For Your Data Privacy?*, PBS (Nov. 1, 2019), https://www.pbs.org/newshour/economy/making-sense/google-bought-fitbit-what-does-that-mean-for-your-data-privacy [https://perma.cc/MZE8-BU29] (illustrating what companies like FitBit can do with the data they collect).

235. *See infra* notes 257-259 and accompanying text; *see also* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 357 (1991) (articulating that collections of facts, on their own, are not copyrightable).

236. *See, e.g.*, United States v. Craft, 535 U.S. 274, 278 (2002) ("A common idiom describes property as a 'bundle of sticks'—a collection of individual rights which, in certain combinations, constitute property.")

237. Aziz Z. Huq, *The Public Trust in Data*, 110 GEO. L.J. (forthcoming 2020) (explaining how the collection of personal data is a side effect of platform use).

238. For an explanation of why data is so difficult to define and therefore own, see Ali Al-Khouri, *Data Ownership: Who Owns 'My Data'*, 2 INT'L J. OF MGMT. & INFO. TECH. 1, 1-2 (2012) (explaining the difficulties in defining data ownership, but conceding that data created through the analysis would belong to the entity performing the analysis). This Article discussed derived data in Part V.A.2.

239. *See* Marc A. Rodwin, *The Case for Public Ownership of Patient Data*, 302 JAMA 86, 87 (2009) ("In most states, the law treats patient medical records as physical property that physicians and hospitals own, but allows patients and insurers access to records."). *See also* Estate of Finkle, 395 N.Y.S.2d 343, 344 (N.Y.Sur. 1977) ("The vast majority of states hold 'that medical records are the property of the physician or the hospital and not the property of the patient.'") (quoting Gotkin v. Miller, 379 F.Supp. 859, 866-67 (E.D.N.Y.1974), aff'd. 514 F.2d 125 (2d Cir. 1975)); Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 681 U. ILL. L. REV. 707-08 (2007) ("It is generally accepted that doctors own the medical records they keep about patients."). New Hampshire is the only state that gives patients ownership rights in their medical records. Amy L. McGuire et al., *Who Owns the Data in a Medical Information Commons?*, 47 J.L., MEDICINE & ETHICS 62, 65 (2019).

240. U.S. DEP'T OF HEALTH AND HUMAN SERVICES, HEALTH INFORMATION PRIVACY BEYOND HIPAA: A 2018 ENVIRONMENTAL SCAN OF MAJOR TRENDS AND CHALLENGES, at 13-15

patients have a very limited right to control with whom their medical data is shared.[241] Because wearable devices are provided with a license agreement to users, the terms of the license or privacy policy will govern who owns the data and how it can be used.[242] Teams may require players to utilize wearables. Unions may contract with team management to limit the use of the data from the wearables. However, in terms of ownership, there remains the issue that facts themselves cannot be owned.[243]

In the EU, although the GDPR does not directly address ownership of data issues, its robust level of control over personal data that individuals possess under the law are often considered akin to "ownership."[244] Concerning medical data, like in the U.S., healthcare providers do not need a patient's permission to share medical records for research purposes (provided patient confidentiality is protected).[245]

With the arrival of the GDPR, the privacy policies of many wearable companies were modified.[246] A privacy policy is an agreement between the data subject and the collector of data. Because the GDPR granted many rights to data subjects, these companies' privacy policies needed to reflect these new sights and obligations.[247] One of the most important rights is the right of deletion, meaning an individual has the ability to ask the wearable company to delete all of the data they have collected about them (with certain exceptions).[248] With an Apple

---

(Dec. 13, 2017), https://ncvhs.hhs.gov/wp-content/uploads/2018/05/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf [https://perma.cc/2P4M-Q8XW].

241. *Id.*

242. *See* Frazee, *supra* note 234.

243. Ryan M. Rodenberg, John T. Holden & Asa D. Brown, *Real-Time Sports Data and the First Amendment,* 11 WASH. J.L. TECH & ARTS 63, 83 (2015) ("Facts are not copyrightable expressions because they are considered to be in the public domain.").

244. *See* Luke Irwin, *The GDPR: What Exactly is Personal Data*, IT GOVERNANCE (Nov. 12, 2020), https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data [https://perma.cc/C9QD-4CCG].

245. AIMED News, *Medical Data: Who Owns It and What Can Be Done to It?*, AIMED (Oct. 9, 2018), https://ai-med.io/medical-data-artificial-intelligence/ [https://perma.cc/KL6P-UXAX].

246. *See, e.g.*, Kari Paul, *'Tossed My Fitbit in the Trash': Users Fear for Privacy After Google Buys Company*, GUARDIAN (Nov. 6, 2019), https://www.theguardian.com/technology/2019/nov/05/fitbit-google-acquisition-health-data#:~:text=2%20years%20old-,'Tossed%20my%20Fitbit%20in%20the%20trash'%3A%20users%20fear,privacy%20after%20Google%20buys%20company&text=In%20a%20blogpost%20following%20the,trust%20is%20paramount%20to%20Fitbit [https://perma.cc/BL9C-679W] (discussing the impact of the GDPR on Fitbit and users).

247. *Id.*

248. *See generally Your Right to Get Your Data Deleted*, INFO. COMM'R OFF., https://ico.org.uk/your-data-matters/your-right-to-get-your-data-deleted/ [https://perma.cc/N77U-7RLZ] (describing an individual's rights regarding the "right to erasure" under the GDPR).

Watch, the wearer can delete their data from the watch directly.[249] However, the watch also shares the personal data with its affiliates and can combine it with other information it has about the wearer.[250] Fitbit also makes it easy to delete an individual's data, although they maintain the right to sell the de-identified data.[251] In the U.S., on the other hand, there are no restrictions on Apple or Fitbit or any wearable company beyond complying with their own privacy policies.[252] Google's recent purchase of Fitbit makes it very likely that data collected from wearables will be added to personal profiles for advertising, at the very least, and potentially for much more.[253] This issue has yet to be resolved, as in the U.S. (unlike in the EU), a wearer does not have the right to consent to the collection, sharing, and use of their data. Thus, the only option to prevent wearable data from being shared or sold is to stop using the device.[254] While players may have some limited control over their raw data, it is unlikely that they would "own" it under U.S. law.[255] Additionally, any reports created from the analysis of a player's raw data would be derived data and most likely owned by the entity performing the analysis.

2. *Derived Data*

Derived data is information "produced from other data."[256] This is an important feature with respect to data ownership and is, in a sense, the meaning ascribed to data collected. A heart rate at a certain point of time is a data point ("raw data"). The interpretation of the monitoring of an athlete's heart rate over time can reveal information such as

---

249. *Erase Apple Watch*, APPLE, https://support.apple.com/guide/watch/erase-apple-watch-apd4ad3571d9/watchos#:~:text=Open%20the%20Settings%20app%20on,Apple%20Watch%2C%20choose%20Erase%20All [https://perma.cc/3K6J-UFPS].

250. Sophie Charara & Husain Sumra, *We Read Your Wearable Tech's Privacy Policy so You Don't Have To*, WAREABLE (May 25, 2018), https://www.wareable.com/wearable-tech/terms-and-conditions-privacy-policy-765 [https://perma.cc/2XZ7-MPDJ].

251. *Id.*

252. *See, e.g.*, Mark Weinstein, *What Your Fitbit Doesn't Want You to Know*, HUFFPOST (Dec. 21, 2015, 5:53 PM), https://www.huffpost.com/entry/what-your-fitbit-doesnt-w_b_8851664 [https://perma.cc/CE6Z-QLXP].

253. Thorin Klosowski, *Lots of Health Apps Sell Your Data. Here's Why*, LIFE HACKER (May 9, 2014, 1:00 PM), https://lifehacker.com/lots-of-health-apps-are-selling-your-data-heres-why-1574001899 [https://perma.cc/9LP3-M3MW] ("In a recent study, the FCC studied 12 different health and fitness apps and found they sent data to 76 different third parties. This data included names, email addresses, exercise habits, diets, medical symptom searches, location, gender, and more.").

254. *See generally* Gretchen Frazee, *Google Bought Fitbit. What Does That Mean for Your Data Privacy?*, PBS (Nov. 1, 2019, 7:03 PM), https://www.pbs.org/newshour/economy/making-sense/google-bought-fitbit-what-does-that-mean-for-your-data-privacy [https://perma.cc/RLA7-WK56].

255. Because "facts" cannot be owned under U.S. copyright law and patients do not own their medical records, it is unlikely that raw data would be owned by the data subjects from whom it is collected. *See supra* notes 235-245 and accompanying text.

256. KITCHIN, *supra* note 62, at 1.

a heart condition requiring medical intervention ("derived data"). The speed with which an athlete runs at a single point in time is a data point ("raw data"). Monitoring and analyzing an athlete's speed over time can indicate a reduction in skill ("derived data"). It is the derived data that presents the greatest risks but also contains the most value. The question that arises is: who owns derived data? Is it the athlete whose data points were collected, the team which authorized the analysis, or the device maker that collected and analyzed the data and thus created the derived data?

Overall, ownership of derived data is an up-and-coming issue as the value of the data resulting from the implementation of the IoTs becomes apparent. Although common law ownership rights do not currently exist, parties can allocate the ownership and use of different categories of data through contract law.

Under U.S. intellectual property law, facts are not protectable.[257] Sports scores, for example, cannot be "owned."[258] In *Feist Publications, Inc. v. Rural Telephone Services Co.*, the Supreme Court stated that "all facts—scientific, historical, biographical, and news of the day. . . . [']may not be copyrighted and are part of the public domain available to every person.' "[259] The idea that one could own biometric information requires a new way of thinking about what that data is and how it is created. Because ABD includes health data in addition to performance data, additional legal and ethical issues come into play. There is a tension, for example, between an emphasis on patient privacy and the desire for medical data to support research in the interest of public health.[260] The reason for the lack of regulation providing patients with ownership of their own PHI is the enormous benefits of discoveries by researchers who analyze such data.[261] For example, although HIPAA protects the privacy of a patient's medical records, it does not grant any ownership of their own records rights to individuals.[262] While the

257. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 348 (1991).

258. NBA v. Motorola, Inc., 105 F.3d 841 (2d Cir. 1997).

259. *Feist*, 499 U.S. at 348 (quoting Miller v. Universal City Studios, Inc., 650 F.2d 1365, 1369 (CA5 1981) (ruling that names and addresses in a phone book were merely information and could not be protected by copyright law)).

260. Daniel Wartenberg & W. Douglas Thompson, *Privacy Versus Public Health: The Impact of Current Confidentiality Rules*, 100 AM. J. OF PUB. HEALTH 407, 407 (2010) (stating "recent concerns about identify theft, confidentiality, and patient privacy have led to increasingly restrictive policies on data access, often preventing researchers from using these valuable data. We believe that these restrictions, and the research impeded or precluded by their implementation and enforcement, have had a significant negative impact on important public health research.").

261. *See* LAWRENCE O. GOSTIN ET AL., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH (2009), https://www.ncbi.nlm.nih.gov/books/NBK9579/ [https://perma.cc/PG3P-WGZS] (discussing the value of health information privacy).

262. *Who Owns Health Information?*, HEALTHINFOLAW.ORG (Aug. 2015), http://www.healthinfolaw.org/lb/download-document/6640/field_article_file [https://perma.cc/R4T2-AA8F].

research benefit to ABD is different, this bias against health data ownership influences current U.S. law.[263] Whereas the initial data may not be sensitive, such as a player's speed, what can be inferred might be, such as a sudden decrease in speed over a short period of time (indicating health problems).[264] Today, artificial intelligence can run algorithms on this data to create reports combining various data points (this new data is considered derived data) and make predictions.[265] The rationale for protecting derived data differs from protecting the underlying data. Additionally, while the players "provide" the underlying data, it is the algorithms that create the derived data. This, combined with issues related to medical versus non-medical data, creates challenges surrounding the application of property law.

Personal property law generally falls under state common law, except for intellectual property which mostly falls under federal law. While proposals have been made to permit the sale of personal data,[266] that is not currently the framework in the U.S.[267] There are, however, companies that serve as a middleman between individuals and the researchers and companies that desire to use their information for a

263. However, after the story of Henrietta Lacks became public, states began creating laws to provide some ownership rights to an individuals' medical data. Henrietta Lacks was a member of an underrepresented minority group whose cancer cells were used by her doctors to form a multi-billion-dollar industry and who provided her with no compensation. Jorge L. Contreras, *The False Promise of Health Data Ownership*, 94 N.Y.U. L. REV. 624, 627 (2019) (states creating ownership rights included Alaska, Colorado, Georgia, Louisiana, and Florida).

264. *See* Sheri B. Pan, Note, *Get to Know Me: Protecting Privacy and Autonomy Under Big Data's Penetrating Gaze*, 30 HARV. J.L. & TECH. 239, 247 (2016) ("Big data is capable of using innocuous data about a person to make inferences of a sensitive nature.").

265. John Murphy, *This Calculator Will Predict When You'll Die*, MDLINX (May 3, 2019), https://www.mdlinx.com/internal-medicine/article/3685 [https://perma.cc/62E3-GVCE] (describing the Healthy Life Expectancy Calculator created at the University of Connecticut's Janet and Mark L. Goldenson Center for Actuarial Research).

266. Noam Kolt, *Return on Data: Personalizing Consumer Guidance in Data Exchange*, 38 YALE L. & POL'Y. REV. 77, 79 (2019) ("Brittany Kaiser, former Director of Business Development at Cambridge Analytica, provocatively declared that '[p]rivacy doesn't exist in a post-Facebook crisis era . . . . Just like with Airbnb – if somebody is going to come and use your physical assets, you would expect to agree [on] a price and what they're going to do with it before you hand over the keys to your house . . . . Why isn't it the same with your data?' ") (citing Michelle Jamrisko & Mark Miller, *If Privacy Is Dead, Some Argue People Should Sell Their Own Data*, BLOOMBERG (Sept. 6, 2018), https://www.bloomberg.com/news/articles/2018-09-06/if-privacy-is-dead-some-argue-people-should-sell-their-own-data [https://perma.cc/FGZ8-TW9Y]).

267. The concept of being able to control one's personal data is generally more accepted in Canada and the EU. Both regions have strong data protection laws which allow individuals more control over their data than is available in the U.S. *See* Teresa Scassa, *Data Ownership*, CTR. FOR INT'L GOVERNANCE INNOVATION 1, 1-3 (2018), https://www.cigionline.org/sites/default/files/documents/Paper%20no.187_2.pdf [https://perma.cc/4NBU-PXX2]. *See also* Kimberly A. Houser & Debra Sanders, *The Use of Big Data by the IRS: Efficient Solution or the End of Privacy as We Know It?*, 19 VAND. J. ENT. & TECH. L. 817, 866 (2017) (describing how the law has not kept up with developments in technology creating large gaps in data privacy and protection).

fee.[268] Due to the Cambridge Analytica scandal,[269] many people now understand that data is a commodity and that companies collecting it (such as Facebook or Google) sell access to it. Fewer understand the model that exchanges free services for your data.[270] Still, fewer realize that their Apple Watch and Fitbit data have value beyond their personal use.[271]

Arguments for ABD ownership can be made under several legal theories: (1) copyright compilation, (2) trade secret, and (3) contract law. Each has its limitations, although all are instructive in understanding the unique legal issues surrounding ABD.

B. Copyright Compilation

Although copyright protection will most likely not apply to the underlying data collected, the report generated from the data could potentially be protectable under a theory of copyright compilations. Under copyright law, ideas may not receive protection, only work put into final form.[272] As previously discussed, facts themselves may not be protected.[273] However, some have made a case for derived data to be protected as a "compilation."[274] The argument is that the selecting and arranging of certain data (as with an analytics program) creates a compilation because of the originality of the selection and arrangement.[275] The author of the compilation is generally different from the source of the data.[276] In other words, while the source of the data is the athlete, the report produced from the analysis of data would be the

---

268. Contreras, *supra* note 263, at 625-27.

269. *See* Alvin Chang, *The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram*, VOX (May 2, 2018, 3:25 PM), https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram [https://perma.cc/JY8D-GR2N].

270. Kimberly A. Houser & W. Gregory Voss, *Can Facebook and Google Survive the GDPR?*, U. OXFORD: OXFORD BUS. L. BLOG (Aug. 29, 2018), https://www.law.ox.ac.uk/business-law-blog/blog/2018/08/can-facebook-and-google-survive-gdpr [https://perma.cc/HM6R-B6PB].

271. *Healthcare Analytics Market Worth $75.1 Billion by 2026*, MARKETSANDMARKETS.COM, https://www.marketsandmarkets.com/PressReleases/healthcare-data-analytics.asp [https://perma.cc/R4YH-VYXW] (estimating the future value of health care data at $75 billion).

272. 17 U.S.C. § 102(a) (2012) (stating that "copyright protection subsists . . . in original works of authorship fixed in any tangible medium of expression").

273. *See supra* notes 257-259 and accompanying text.

274. CCC Info. Servs., Inc. v. MacLean Hunter Mkt. Reports, Inc., 44 F.3d 61, 67 (2d Cir. 1994) (finding that the "selection and arrangement of data in [a valuation book] displayed amply sufficient originality to pass the low threshold requirement to earn copyright protection" because it contained more than "pre-existing facts" and instead included predictions "based not only on a multitude of data sources, but also on professional judgment and expertise" unlike the "telephone numbers in Fiest"); Elvy, *supra* note 149.

275. Scassa, *supra* note 267, at 6.

276. *Id.* ("[F]or example, the creator of an anthology of stories is not typically the author of the stories it contains[.]").

"compilation." As scholar Teresa Scassa explains, the originality component required in order to receive copyright protection would be the combinations and analysis of various data points.[277]

The problem with this argument is that under current law only works created by humans can be copyrighted.[278] In other words, works created by computers running algorithms cannot.[279] Circular 31, from the U.S. Copyright Office, states: "Copyright law does not protect ideas, methods, or systems. Copyright protection is therefore not available for ideas or procedures for doing, making, or building things; scientific or technical methods or discoveries; business operations or procedures; mathematical principles; formulas or *algorithms*; or any other concept, process, or method of operation."[280] Part of the challenge with laws in the U.S. is that Congress lacks an understanding of technology, making it very difficult for them to address the issues involved.[281] Additionally, much of the law impacting technology was created prior to widespread public internet use and advanced data analytics.[282] We expect this issue to be brought to the forefront soon, both in the U.S. and abroad. Google has developed AI that can write news articles and create music, and a consortium of museums and researchers in the Netherlands can create artwork based on data points collected from Rembrandt paintings.[283]

One of the cited flaws in the U.S. Copyright Office's stance on ownership is that they ignore the creativity involved in the creation of an algorithm.[284] Various decisions go into the process such as deciding what the algorithm will examine (or what problem it will solve),

277. *Id.*

278. According to Section 306 of the Compendium of U.S. Copyright Office Practices, "The Human Authorship Requirement": "The U.S. Copyright Office will register an original work of authorship, provided that the work was created by a human being. The copyright law only protects 'the fruits of intellectual labor' that 'are founded in the creative powers of the mind.' . . . [As such,] the Office will refuse to register a claim if it determines that a human being did not create the work." *See Compendium of the U.S. Copyright Office Practices: Chapter 300*, U.S. COPYRIGHT OFF. (Jan. 28, 2021), https://www.copyright.gov/comp3/chap300/ch300-copyrightable-authorship.pdf [https://perma.cc/R8HP-E8N5] (citation omitted). *See also* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 348 (1991) (indicating that copyright law only protects " *'the fruits of intellectual labor'* " that " 'are founded in the creative powers of the mind' ").

279. *Ideas, Methods, or Systems,* U.S. COPYRIGHT OFF. 1 (Jan. 2012), https://www.copyright.gov/circs/circ31.pdf [https://perma.cc/QBP6-DS7B].

280. *Id.* (emphasis added).

281. *See, e.g.*, Shira Ovide, *Congress Doesn't Get Big Tech. By Design,* N.Y. TIMES (July 29, 2020), https://www.nytimes.com/2020/07/29/technology/congress-big-tech.html [https://perma.cc/P8GG-BNVS] (describing Congress' failure to understand Facebook).

282. *See* Christina Delgado, *Will Congress Finally Update a Data Privacy Law That's 31 Years Old?*, WASH. EXAMINER (Sept. 13, 2017, 1:01 PM), https://www.washingtonexaminer.com/will-congress-finally-update-a-data-privacy-law-thats-31-years-old.

283. Andres Guadamuz, *Artificial Intelligence and Copyright*, WIPO MAGAZINE (Oct. 2017), https://www.wipo.int/wipo_magazine/en/2017/05/article_0003.html [https://perma.cc/ZBR5-9D5V].

284. Scassa, *supra* note 267, at 6.

selection and cleaning of data sets, categorization (or labeling) of the data, the steps the algorithm needs to complete, and reviewing the output and refining the algorithm. Humans complete these steps.[285] The use of a computer is comparable to the use of other tools, such as those found in a recording studio. Scholars have addressed this issue under different theories. Kalin Hristove makes a case for copyright ownership in his piece, *Artificial Intelligence and the Copyright Dilemma,* arguing that the law does not need to be changed to allow non-human ownership of AI-generated works, but rather apply the "work made for hire" paradigm as providing ownership to the programmer or owner of the AI.[286] One could also argue that derived data using an algorithm to make predictions based on input data is protectable under copyright law.[287]

Scholar Samantha Fink Hedrick makes a cogent argument that AI-generated works can be owned by the human that created the algorithm.[288] She argues that those creating the algorithm maintain enough control over the algorithm's steps to be considered human decisions.[289] By designing the algorithm itself, the human is engaging in a creative process.[290] She makes the analogy that, "[l]ike a camera, AI functions merely as a tool of creation, not as a sentient 'author.' "[291]

The issue with athlete ownership of ABD is that the athlete is the source of the raw data, which is not protected by copyright law. There is no known law that protects one's running speed or heart rate at a particular point in time, as the law treats each as "facts" or "information."[292] The law considers facts to be in the public domain, meaning

285. Except in the case of machine learning, where a computer may review and refine an algorithm without human input. Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARV. J.L. & TECH. 889, 891 (2018) (explaining that machine-learning algorithms are "capable of learning from massive amounts of data, and once that data is internalized, they are capable of making decisions experientially or intuitively like a human"). However, humans would most likely be involved in the rest of the steps. Although it is possible that less and less human input could be involved, further muddying the issue. *See id.* at n.8 ("[M]odern AI can arrive at solutions or solve problems without the need for a human programmer to specify each instruction needed to reach the given solution. Thus, AI may solve a particular problem or reach a solution that its programmer never anticipated or even considered.").

286. Kalin Hristov, *Artificial Intelligence and the Copyright Dilemma*, 57 IDEA 431, 449 (2016).

287. *See* BanxCorp v. Costco Wholesale Corp., 978 F. Supp. 2d 280, 305 (S.D.N.Y. 2013) (suggesting that factual data is not a protectable under copyright law, although hypothetical data could be [the actual price of a car versus the projected price of a car]).

288. *See* Samantha Fink Hedrick, *I "Think," Therefore I Create: Claiming Copyright in the Outputs of Algorithms*, 8 N.Y.U. J. INTELL. PROP. & ENT. L. 324, 324 (2019).

289. *Id.* at 328-29.

290. *Id.*

291. *Id.* at 325 (emphasis omitted).

292. Determann, *supra* note 59, at 11 n.54 ("Patent law excludes laws of nature, natural phenomena and abstract ideas from patentable subject matter.") (citing Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66, 70-71 (2012)) ("Trademark law denies

that anyone can reproduce facts without running afoul of copyright law. Additionally, even if the report or output from analytics running on these underlying data points could be protected, the copyright protection would only extend to the output, not the underlying data.[293]

Other scholars have noted that copyright law is a weak way to establish ownership of personal data and that the new rise of the big data economy requires new laws.[294] Another potential area for protecting biometric data is through trade secret law.

C. *Trade Secret*

Under U.S. law, a "trade secret" is any information which has (1) "independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information[,]" and (2) which "the owner thereof has taken reasonable measures to keep such information secret."[295] Trade secret law is different from copyright law because an individual can have an ownership interest in the copyrighted material.[296] Trade secret law permits one to keep their information confidential and provides remedies if the information is stolen.[297] It does not create ownership, but rather assumes it.[298] It gets around the ownership issue by creating a way to monetize the information.[299] Customer databases, for example, have historically been protected by trade secret law.[300] The idea is that the value of the information "lies in its confidentiality, and not in the information itself."[301] For example, if the information at issue is how many years of play an athlete has left based on her physical

---

protection for generic marks.") (citing Park 'n Fly v. Dollar Park & Fly, 469 U.S. 189, 194 (1985)) ("Copyright law excludes facts and ideas from copyright protection.") (citing 17 U.S.C. § 102(b) (2012)).

293. Scassa, *supra* note 267, at 1 ("In the European Union, database rights offer a more robust protection for compilations of data, but they also fall short when it comes to protecting the facts that make up such compilations.").

294. Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 222 (2018) (arguing that big data sets have nothing to do with the original intent of copyright law which is to protect creative works); Sylvia Zhang, *Who Owns The Data Generated By Your Smart Car?*, 32 HARV. J.L. & TECH. 299, 305 (2018) ("Existing intellectual property regimes such as patent, trademark, and copyright do not apply well to the ownership of data.").

295. *See* 18 U.S.C. § 1839(3) (2016).

296. Deepa Varadarajan, *Trade Secret Precautions, Possession, and Notice*, 68 HASTINGS L.J. 357, 362-66 (2017) (providing an overview of trade secret law).

297. *Id.*

298. *Id.*

299. *Id.*

300. Elvy, *supra* note 149, at 471.

301. Scassa, *supra* note 267, at 12.

condition, the value comes from keeping this information private. This information would have value to different entities in contract negotiations, trades, and matches.

What is important to remember is that when a third party collects ABD and provides reports to the player, the team, and the team's doctor, all of these parties have different interests in that data. The source data (heart rate, speed) are facts, with the player having no ownership rights under common law. The player, however, would want to, at the very least, protect this information from disclosure. This is a different issue than commercializing data, and a different issue than protecting predictions or reports made from a compilation of the source data, and that is what makes this issue so difficult to address.

The rationale behind trade secret protection is that entities that invest significant time and money into the creation of databases should be able to protect them against misappropriation.[302] Although an entity cannot claim ownership in facts, trade secret law provides a remedy for the theft or unlawful disclosure of the "arrangement of facts."[303]

Like the copyright argument, the trade secret theory also has some problems. First, in the U.S., trade secret law exists primarily under fifty different state laws modeled on the Uniform Trade Secrets Act.[304] Additionally, because trade secrets are not exclusive and are not registered, more than one entity can claim ownership if developed independently.[305] This permits others to create similar analytics programs and create similar reports from data in the public domain. Thus, because one team claims ownership of certain information as subject to trade secret law does not prevent another team or entity from creating the same information.

D. Contracts

Several recent developments have helped to address the issue of the biometric monitoring of professional athletes who are subject to labor agreements. In 2015, the NFL began using Radio-frequency identification (RFID) chips to track its players' and the ball's movement

---

302. Determann, *supra* note 59, at 21.

303. *See id.*

304. *See* Brittany S. Bruns, *Criticism of the Defend Trade Secrets Act of 2016: Failure to Preempt*, 32 BERKELEY TECH. L.J. 469, 473-80 (2017) (describing the history of trade secret law in the United States).

305. The federal Defend Trade Secrets Act merely allows companies to move these disputes into federal court. *See* 18 U.S.C. § 1838 (1996) ("Except as provided in section 1833(b), this chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act).").

during games.[306] These RFID radio chips work like the ones embedded in pets to track their location if they get lost, or like the chips in toll cards affixed to a car windshield. The chip transmits data through radio waves to the antenna, where the chip is identified, and information is analyzed.[307] In the case of a pet RFID, the RFID reader can obtain the owner's contact information.[308] With a toll RFID card, as the car passes through the toll booth, a reader can identify the account associated with the card and deduct the amount of the toll from the owner's account.[309] The RFID chips used in football are inserted into the players' shoulder pads, and in addition to tracking location, they also track speed and other metrics.[310] Although the data collected was initially shared with the players and their coach only, in 2018, the NFL decided to make that data available to all of the teams in the NFL.[311]

Unlike online user agreements where there is little ability to negotiate what data may be collected and how it can be used, many athletes are subject to collective bargaining agreements, which may be the best route to gain commercial rights to derived data created from an athlete's raw biometric data.[312] In general, these contracts provide that data collected during practice belongs to the teams, and data collected during the games belongs to the league.[313] Much of it comes down to the contract between the provider of the device and the team or league that contracts with them.[314] Issues get muddied when players are traded or if the contracts do not limit what the wearable entity can do with the data.

---

306. Ian McMahan, *The Tricky Ethics of the NFL's New Open Data Policy*, WIRED (Mar. 29, 2018, 8:00 AM), https://www.wired.com/story/the-tricky-ethics-of-the-nfls-new-open-data-policy/ [https://perma.cc/5HVG-V4MN].

307. *Radio Frequency Identification (RFID)*, U.S. FDA, https://www.fda.gov/radiation-emitting-products/electromagnetic-compatibility-emc/radio-frequency-identification-rfid [https://perma.cc/7NV2-2JGW] (last visited Jan. 13, 2022).

308. *See Microchipping of Animals FAQ*, AM. VETERINARY MED. ASS'N, https://www.avma.org/microchipping-animals-faq [https://perma.cc/K5A3-WBC7] (last visited Jan. 13, 2022).

309. *See* Josef Czako, *Where is Tolling Tech Taking Us?*, ITS INT'L (Sept. 25, 2019), https://www.itsinternational.com/its1/feature/where-tolling-tech-taking-us [https://perma.cc/SSL2-C47N].

310. McMahan, *supra* note 306.

311. Some have pushed back against this use of data as changing the very nature of football and hypocritical of rules preventing filming other teams' practices, using advanced hearing devices to hear plays being called, and using a camera phone to track another team's signs. *See id.* ("'In sports, we want talent, dedication and effort to be difference makers, so how much do we want technology to decide the outcome of games?' asks Thomas Murray, president emeritus of the Hastings Center, a prominent ethics research center. 'Taking the human element out of the game, making it a competition among scientists rather than athletes, does seem to undermine what we value in sport,' says Murray, who wrote about the ethics of performance enhancement in his book *Good Sport*.").

312. *See supra* Section III.B.

313. *Id.*

314. *See* NBA–NBPA Collective Bargaining Agreement, *supra* note 105, at 359-61.

Additional protections are necessary for student athletes who cannot negotiate terms related to their ABD. Although college athletes do not have a player's union per se that can negotiate ABD ownership rights for them, they are in a unique position regarding their legal classification due to a push for the National Collegiate Athletic Association (NCAA) to change its policy on player's right to monetize their name, image, and likeness.[315] States are beginning to look at passing "pay to play" laws allowing collegiate athletes to capitalize on the sale of their name, image, and likeness rights.[316] The California bill, which passed 112-0, would allow college athletes to commercialize their image beyond university gates by law, effectively preempting NCAA policy.[317] The law, which is to take effect in 2021, still has several questions surrounding its implementation, including how the NCAA will respond. Athletes at the collegiate level may be able to individually or collectively commodify their ABD.[318] It would likely be financially advantageous if athletes were able to collectively sell their ABD, as opposed to each individual athlete selling access, as the commercial desirability for a single athlete's data is likely nominal. Given the limitations of collective bargaining agreements for professional athletes and the lack of any collective agreements for college athletes, individual contractual agreements may not be the best avenue to address the concerns raised in this paper.

---

315. *See* Dan Murphy, *What California Bill Means for NCAA Image and Likeness Debate*, ESPN (Oct. 1, 2019), https://www.espn.com/college-football/story/_/id/27585301/what-california-bill-means-ncaa-image-likeness-debate [https://perma.cc/7T9G-8ERV]; Nancy Skinner & Scott Wilk, *In California, We Forced the NCAA's Hand on Paying Athletes. But More States Must Step Up*, USA TODAY (Jan. 16, 2020, 1:09 PM), https://www.usatoday.com/story/opinion/2020/01/15/ncaa-california-student-athletes-pay-image-likeness-column/4456723002/ [https://perma.cc/Y7EP-DPYB] ("The NCAA, colleges and universities, and TV networks have pocketed hundreds of millions of dollars while athletes — the people most responsible for generating all that wealth — have been denied the right to share in the riches. And public opinion couldn't be clearer. Polls show that Americans are increasingly in favor of college athletes having the right to be compensated based on their name, image and likeness.").

316. Colorado, Florida, Illinois, Kentucky, Minnesota, Nevada, New York Pennsylvania, South Carolina, and Washington all have similar bills pending. Additionally, Anthony Gonzalez, R-OH, a former Ohio State University wide receiver, wants to introduce a bill at the federal level giving college athletes the right to their name, image, and likeness. Matt Norlander, *Fair Pay to Play Act: States Bucking NCAA to Let Athletes Compensation for Their Name, Image, Likeness*, CBS SPORTS (Oct. 3, 2019, 5:43 PM), https://www.cbssports.com/college-football/news/fair-pay-to-play-act-states-bucking-ncaa-to-let-athletes-be-paid-for-name-image-likeness/ [https://perma.cc/UKM3-EGH7].

317. *California Senators to Introduce Supplement to SB 206 in Advance of NCAA's January Name, Image, Likeness Vote*, NAT'L L. REV. (Dec. 8, 2020), https://www.natlawreview.com/article/california-senators-to-introduce-supplement-to-sb-206-advance-ncaa-s-january-name [https://perma.cc/FV2S-LLB8]; *see* Murphy, *supra* note 315.

318. Murphy, *supra* note 315.

VI. RECOMMENDATION—DATA TRUST

Privacy and data ownership are key concerns when considering an athlete's ABD. Privacy protections can help prevent discrimination, adverse employment action, and provide the data subject with the ability to control with whom the data is shared. Ownership of ABD clarifies who can monetize the data and who can determine its use. The exact nature and legal status of ABD is difficult to determine because it can include an individual player's PHI (e.g. injury information); raw data (e.g. running speed), which cannot be owned; and/or derived data (e.g. a report on improvement in speed or strength over time), for which the manufacturer of the device collecting the data claims ownership.

Because of the conflicting objectives regarding ABD among the leagues, universities, players, and device makers, as well as the potential risks of espionage and gaming harms, neither a new statute nor a bilateral contract will be sufficient to address the needs of all. In addition to risks, there are both public and private benefits of access to ABD. For example, a team may be able to address a player's health concerns, prevent injuries, maximize training efficiency, and provide the team with a better understanding of an athlete's capabilities.[319] A data trust also has the unique advantage of potentially providing anonymized medical and performance data to institutions for research, which could be of enormous value to society. For example, allowing access to this data could lead to advances in concussion protocols or chronic traumatic encephalopathy.[320] Rather than a model of ownership of ABD, we propose that a data trust can address what calls for ownership rights seek to resolve—namely, controlling the use of data; addressing the risks in sharing data; and monetizing data.

A. What Is a Data Trust?

Although originally conceived in Nobel Prize Winner Elinor Ostrom's 1990 seminal work, *Governing the Commons*,[321] the concept of governance structures, known as commons, has received renewed interest as being applicable to data.[322] Data trusts, a type of commons

---

319. Sanyal, *supra* note 39.

320. *See generally* Mansi Vakil, *Data Collection: A Huge Step Towards Tracking Brain Injury*, CONCUSSION TALKS (Aug. 24, 2019) (on file with authors).

321. ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (1990) (suggesting a commons governance scheme for managing common pool (finite) resources such as grazing land, forests, and irrigation waters).

322. Anouk Ruhaak, *Data Trusts and Data Commons*, MEDIUM (May 15, 2020), https://medium.com/@anoukruhaak/data-commons-data-trust-63ac64c1c0c2 [https://perma.cc/JA3Q-9TJX]. With respect to common pool resources, "[Ostrom's] research found that communities often find ways to decide on access to and use of the resource between themselves. These are commonly referred to as commons." *Id.* Although data is not a

governance structure, can address the issues arising from the lack of sufficient regulations regarding the use of data. An important foundational aspect to shared governance, as such data trusts create, is that those whose data is being used should have a say in the rules regarding such use.[323] These fiduciary data trusts are an agreement that sets up a board representing the interests of impacted stakeholders for the purpose of governing the collection, use, and potential commoditization of data.[324] While many suggestions for the use of data trusts center on data gathered from smart cities,[325] a data trust could be utilized for ABD collected from players by device makers. As scholars Wylie and McDonald explain, "Beyond providing the structure of fiduciary governance, data trusts can act as a way for data rights holders to aggregate and build leverage toward collectively bargaining for more balanced, publicly beneficial data relationships."[326] As a report for the Province of Ontario, Canada explained, current methods are insufficient to address the issues relating to the collection of data in smart cities:

> The mix of public and private sector actors leads to potentially conflicting data access and ownership rights; a lack of standardized technical architecture; and varying levels of control, communication, and transparency to citizens. A lack of standards and large data assets held by only a few actors could skew the benefits from economic development, while leaving other needs like security, privacy, and social equity unmet.[327]

We see similar issues with the use of biometric data. The data trust framework has an advantage over bilateral agreements (which do not consider all parties impacted) by allowing the *ab initio* creation of a

---

common pool resource, it does share characteristics in that certain parties may be able to legally exclude others from accessing the data. *Id. See* Richard Kemp, *Data Trusts and Frameworks are Gaining Traction and on the Cusp of Widespread Adoption*, LEXOLOGY (Sept. 2, 2019), https://www.mondaq.com/uk/data-protection/842350/data-trusts-and-frameworks-are-gaining-traction-and-on-the-cusp-of-widespread-adoption [https://perma.cc/B4WL-B243] ("[D]ata trusts . . . appear to be on the cusp of widespread adoption with great potential as a practical and workable way forward [to address data sharing issues in the face of the explosive growth of data collection].").

323. Bianca Wylie & Sean McDonald, *What Is a Data Trust?*, CIGIONLINE (Oct. 9, 2018), https://www.cigionline.org/articles/what-data-trust [https://perma.cc/35M2-FYG3].

324. *Id.*

325. *See, e.g.*, Christine Rinik, *Data Trusts: More Data than Trust? The Perspective of the Data Subject in the Face of a Growing Problem*, 34 INT'L REV. L., COMPUTERS & TECH. 342 (2019); Kelsey Finch & Omer Tene, *Smart Cities: Privacy, Transparency, and Community*, *in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 125 (Evan Selinger et al. eds., 2018).

326. Wylie & McDonald, *supra* note 323 (citing Paul B. Miller & Andrew S. Gold, *Fiduciary Governance*, 57 WM. & MARY L. REV. 513 (2015)).

327. *Building Ontario's Next-Generation Smart Cities Through Data Governance*, COMPUTEONTARIO 1, 10, https://www.orion.on.ca/blog/smart-cities-ices/ [https://perma.cc/DC24-WJAJ] (last visited Jan. 14, 2022).

document considering all parties' objectives. Additionally, a data trust may be designed to not only address issues of ownership, but also detail how data may be used, shared, protected, and monetized.

For the purposes of this Article, we define a data trust as an entity with fiduciary responsibility and technical capacity to manage data use rights and ABD assets on behalf of athletes, while also taking into consideration the stakeholders such as leagues, universities, device makers, and those in public health research.[328] A data trust can address the inadequacies of both regulations and contracts regarding data ownership and legal risks.[329]

B. Benefits of a Data Trust

A data trust would address the imbalance of bargaining positions between those from whom data is collected and those who seek to use the data.[330] Scholar Rinik outlines the benefits of a data trust approach:

> Use of a data trust where the beneficiaries are the individual data subjects might help to restore some balance between the needs of data controllers with the interests of the data subjects. The individual often has no voice in the creation of frameworks for the protection of personal data and the limits on the power of the data controllers.[331] If the data subject is treated as a beneficiary of the data trust this may give them more of a voice in the processing of their data and address the power imbalance that has been created in the market for data.[332]

Additionally, data subjects would be accountable for the accuracy and completeness of the data generated through the rules of the data trust.[333] This is especially important as AI requires trustworthy data.[334] If the data is inaccurate or incomplete, its usefulness is reduced.[335]

A data trust would enable researchers to access the vast and valuable sets of data to generate insights, which could help identify the

---

328. Modifying the definition given in Finch & Tene, *supra* note 325, at 126-27 n.10.

329. Sylvie Delacroix & Neil Lawrence, *Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, 9 INT'L DATA PRIVACY L. 236, 236-37 (2018).

330. DATA TRUSTS: A NEW TOOL FOR GOVERNANCE, ELEMENTAI, https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf [https://perma.cc/E6A4-4X6Z].

331. This is especially true in the United States where there is no national privacy legislation. *See* Houser & Voss, *supra* note 139.

332. Rinik, *supra* note 325, at 21.

333. Chris Reed & Irene Ng, *Data Trusts as an AI Governance Mechanism*, at 2 (Working Paper 2019), https://ssrn.com/abstract=3334527 [https://perma.cc/4FGA-LDS3].

334. *Id.*

335. *Id.*

most effective injury prevention protocols and identify health risks in advance of their manifestation.

C. *Components of a Data Trust*

The creators of the data trust would need to identify the stakeholders and their needs, decide on the management and governance structure of the trust, create systems for the collection, use and sharing of the data, and determine a financing structure to address how various parties are compensated. The following would need to be defined and negotiated akin to a collective bargaining process:

- Definition of data;
- Commodification of data;
- Permitted and prohibited uses of the data;
- Confidentiality of data;
- Security of data; and,
- Licensing of data.

One place to start is with the collective bargaining agreements addressing biometric data collection. Athletes, who are parties to collective bargaining agreements (e.g. professional athletes of team sports in the United States), should first review the wearables language in the NBA's collective bargaining agreement.[336] This language provides a starting point which could be expanded beyond its current focus on wearables, to a full portfolio of biometric data collection.[337] The second step is to define how to treat raw data versus derived data and to allocate the ability to use and commodify such data. We argue that players (or athletes) should be included in determining the scope of what can be done with their biometric data and that this is done on an opt-in basis (not an opt-out basis). Athletes, team owners, and/or the device maker could negotiate the rights between each other through intermediaries.

The data trust entity would consist of a board, including representatives of each of the parties with an interest in the ABD (player, team, device maker). A trust has the added benefit of being able to provide an agreed-upon definition of commodification and address potential public interest uses. Data use could also be addressed in advance, including issues involving player transfers, contract negotiation, sharing of data, potential disability discrimination, location and health privacy, data security, and handling potentially erroneous raw data and derived data.

---

336. NBA–NBPA Collective Bargaining Agreement, *supra* note 105, at 359-61.

337. *Id.*

We also recommend that the data trust include provisions incorporating cybersecurity language endorsed by Grow and Shackelford, who argue for the establishment of league-wide data security protection for wearables, raw data, and derived data collections.[338] This may involve working with wearable manufacturers to enhance the products that professionals use to provide greater security levels than those that are commercially available. Grow and Shackelford also recommend extracting disputes from the purview of the league commissioners' oversight to the oversight of an independent arbitration body capable of reviewing matters, which can easily be provided in the data trust agreement.[339] Indeed, the establishment of an unaffiliated dispute resolution body to address these types of disputes would likely be welcomed by players' associations across sports leagues. Although these recommendations should provide leagues and professional athlete players' associations a framework towards commercializing ABD, at the collegiate level, significant obstacles center on the athletes' status as student-athletes as opposed to employees or independent contractors.[340]

Given ABDs value to multiple parties, it is important to establish, first and foremost, protections for athletes, with respect to use and sharing limitations. It would be a grave mistake to permit the makers of the wearables to commercialize and control how ABD may be used, despite that being the current default due to the lack of uniform federal privacy protections in the U.S. Athletes need to have protections in place from teams, leagues, and device makers who may not have the players' best interests in mind and to permit them to benefit from the monetization of their own ABD. A data trust goes beyond typical privacy and discrimination law and the limits of bilateral contract negotiations, which do not include all impacted parties. It provides a fiduciary framework which protects the athletes while permitting data to be used for the public good. It could serve as a model for how leagues, teams, and device makers may collect, use, and share the ABD and would provide penalties for breaches of the trust.

The trust could also enable the release of ABD, via distribution, similar to the release of injury reports issued by major sports leagues like the NBA, the NHL, and the NFL.[341] Administrators could best determine what information to make available to both media and gambling industry partners; ABD would be within the realm of data that could not be obtained from the public domain, and thus something of

338. Grow & Shackelford, *supra* note 226, at 512-13.

339. *Id.* at 514.

340. *See* Steven L. Wilborn, *College Athletes as Employees: An Overflowing Quiver*, 69 U. MIAMI L. REV. 65 (2014).

341. *See, e.g.*, NAT'L FOOTBALL LEAGUE, 2017 PERSONNEL (INJURY) REPORT POLICY (2017), https://operations.nfl.com/media/2683/2017-nfl-injury-report-policy.pdf [https://perma.cc/63NX-U5D6].

significant value to the gambling industry.[342] The release of standardized and limited ABD information such as training volumes, sleep quality, and training intensity would provide value to those in the gambling industry to more accurately set betting lines.[343] A data trust provides a means for ensuring that athletes are protected while enabling the commercialization of highly sought after information.

CONCLUSION

The collection and commercialization of data is an omnipresent aspect of modern life.[344] The collection of biometric information in the sports world has become one of the most significant tools in the advancement of athlete performance within the last century.[345] The promise that this data holds, however, comes with great risk to the physical, mental, and financial well-being of athletes if misused. There is a highly lucrative gambling market awaiting sale of the data, which requires that protections be put into place to protect the athletes whose bodies are producing the underlying information. Given the shortcomings of patchwork statutes, nonbinding agency guidance, bilateral agreements which exclude some affected parties, and the inability of current law to address all of the risks detailed, the best path forward to mitigate the potential harms to the athletes—while at the same time maximizing the societal and economic value of the ABD—is through the formation of data trusts with multi-stakeholder fiduciary boards that can oversee the implementation and management of all aspects of the handling of ABD.

342. *See* Ethan J. Sanders & Aalok K. Sharma, *Who's on First? – The Fight Over Official Sports Data After* Murphy, STINSON (Mar. 11, 2019), https://www.stinson.com/newsroom-publications-Whos-on-First-The-Fight-Over-Official-Sports-Data-After-Murphy [https://perma.cc/R8NC-F447].

343. *See* Trademate Sports, *How Bookmakers Create Their Odds, From a Former Odds Compiler*, MEDIUM (June 29, 2017), https://medium.com/@TrademateSports/how-bookmakers-create-their-odds-from-a-former-odds-compiler-5b36b4937439 [https://perma.cc/EL3P-ULHW] (describing how bookmakers compile odds).

344. *See, e.g.*, Nitasha Tiku, *What's* Not *Included in Facebook's 'Download Your Data'*, WIRED (Apr. 23, 2018), https://www.wired.com/story/whats-not-included-in-facebooks-download-your-data/ (discussing the wide variety of data collected by Facebook).

345. *See generally* Venook, *supra* note 93.