Nicholas Plinio
SLA Writing Competition
3.20.17

Be-Wear of Wearables: ***Addressing cutting-edge technology and unique data privacy challenges in the "internet age" of professional sports.***

Introduction

In 1999, MIT's Kevin Ashton coined the term "Internet of Things" (IoT) to describe objects embedded with technologies like microchips, sensors, and actuators that use the internet to share data over communication networks.[1] Fast-forward almost twenty years to today's era of internet-enabled innovation, and IoT is poised to revolutionize the way we interact with our world.[2] Among the fastest-growing of these innovations is wearable technology.[3] "Wearables," are a subset of IoT and function as networked devices that can collect data and track the activities of the user.[4] Much of the data collected is classified as "biometric," meaning that it takes the form of "measurable … distinctive physical characteristic[s] or personal trait[s] that can be used to identify an individual."[5] In short, if you have ever used a heart monitor, "fit-bit," or iPhone "Touch Id," you have used a device that has collected your biometric data. This technology has become so popular that global revenue is projected to reach $2.8-billion by 2019.[6] For average consumers, novelty queues the rush to the nearest Best Buy, but experts

[1] Katherine Britton, *IoT Big Data: Consumer Wearables Data Privacy and Security*, American Bar Association (2015), http://www.americanbar.org/publications/landslide/2015-16/november-december/IoT-Big-Data-Consumer-Wearables-Data-Privacy-Security.html#ref5.
[2] Adam Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, 21 RICH. J.L. & TECH. 6, 2 (2015).
[3] *Id.*
[4] *Id.*
[5] COMMENT: FACEBOOK OR FACE BANK?, 32 LOY. L.A. ENT. L. REV. 187, 193 (2012).
[6] Shane Walker, Revenue for Sports, Fitness and Activity Monitors to Increase by Nearly $1 Billion Through 2019, IHS inc. (May. 16, 2014), https://technology.ihs.com/500868/revenue-for-sports-fitness-and-activity-monitors-to-increase-by-nearly-1-billion-through-2019.

attribute the boom in demand to increased use of wearables in professional sports.[7] In fact, as of 2016, every major professional sport in the United States has implemented some form of wearable technology program.[8]

The technology has been met with some enthusiasm, as there is little doubt wearables can revolutionize player development, training, and injury management.[9] However, as with most new and highly disruptive digital technologies, wearable technology challenges existing social, economic, and legal norms.[10] Amid all of the hype, it is easy to forget that the fundamental purpose of these technologies is to collect, store, and disseminate individualized player data. So, while wearable devices might embody some of the decade's greatest innovations, they also represent some of its most hotly contested legal issues: data protection and privacy.

I. Purpose

Few would dispute that athletes have genuine concerns regarding their individual biometric data. Fewer still would argue that there is no place for biometric analysis in sports. However, proper mechanisms for implementation, collection, and use remain unclear. Players fear that negative metrics will manifest themselves in contract negotiation, while organizations champion the benefits to health, safety, and performance.[11] Without an overarching data privacy directive in the United States (like the European Union's General Data Protection Regulation

[7] Stephen Mayhew, Professional sports teams and athletes driving wearable technology, Biometric Update (Oct. 28, 2014), http://www.biometricupdate.com/201410/professional-sports-teams-and-athletes-driving-wearable-technology.
[8] Brian Socolow, *Wearable Tech Will Change Pro Sports - And Sports Law*, Law360 (Sept. 17, 2015), http://www.law360.com/articles/701415/wearable-tech-will-change-pro-sports-and-sports-law.
[9] *See* Katrina Karkazis & Jennifer R. Fishman, *Tracking U.S. Professional Athletes: The Ethics of Biometric Technologies*, 17 THE AM. J OF BIOETHICS 45, 46 (2017).
[10] Thierer, *supra* note 2, at 2.
[11] *See* Joe Lemire, Baseball's Union Remains Wary Of Wearables, Vocativ (Aug. 8, 2016), http://www.vocativ.com/348033/baseballs-union-remains-wary-of-wearables/.

(GDPR), for example), it is challenging to develop a regulatory scheme to balance the interests of both sides.[12]

In the business world, privacy is generally self-regulated through systems of "best practices," focusing on the specific issues facing a given industry.[13] Professional sports are built on self-regulation through Collective Bargaining Agreements (CBA(s)) that manage the relationship between the league, teams, and players. However, while CBAs generally have addressed player privacy, the rate of evolution in this space makes it difficult to tackle issues comprehensively. What guidance we do have suggests that data collected from individuals must adhere to a code of fair practices, including protective mechanisms like subject consent and notice.[14] Moreover, application of these mechanisms seems to be tied directly to the perceived "sensitivity" of the data collected.[15] While I agree that assigning a level of sensitivity is important to establishing a level of security, I propose the need for further assessment—one that looks through the lenses of "intended" and "expected" use. In other words, to assess proper levels of data protection, we must first determine what "uses" the athlete should reasonably expect based on the purpose for collection.

II. General State of Data Privacy Law in the U.S.

When some of today's most recognizable wearables like Fit Bit and Apple Watch first hit the market, many recognized the need for proper safeguards to minimize privacy risks if consumer data were to be used unethically.[16] However, with no single and comprehensive

[12] *See* Socolow, *supra* note 8.
[13] *Id.*
[14] Fed. Trade Comm'n, Privacy Online: Report to Congress ii (1999) [Hereinafter "FTC Report"].
[15] *See* Future of Privacy Forum, Best Practices for Consumer Wearable & Wellness Apps & Devices, 2-3 (2016) [Hereinafter FPF], https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf.
[16] *Id.* at 4.

federal law in this area, coming up with a solution to address the many concerns proved a daunting task for data regulators.[17]

The Federal Trade Commission (FTC)'s "Fair Information Practice Principles" (FIPPs) provide some general guidance with regard to data protection issues.[18] The principles of *Notice*, *Choice*, *Access* and *Security* are designed to "[ensure] that the collection, use, and dissemination of personal information are conducted fairly and in a manner consistent with consumer privacy interests."[19] However, the sophistication of issues posed by modern technology makes the original FIPPs somewhat difficult to apply.[20] According to Adam Thierer, Senior Technology Policy Research Fellow at George Mason University, "[d]ata [from wearables] is going to be moving fluidly across so many platforms and devices that it will be difficult to apply traditional Fair Information Practice Principles . . . Law must still play a role, but we are going to need new approaches.[21] "New approaches" as described by Thierer have generally taken to establishing "baseline" responsible practices that function as "targeted FIPPs" and work alongside federal regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the Americans with Disabilities Act (ADA).[22] However, professional sports present a unique challenge, as the applicability of federal regulations is very unclear.[23]

A. Data Sensitivity and the Health – Lifestyle Distinction

[17] Thierer, *supra* note 2
[18] *Id.*
[19] *See* FTC Report, *supra* note 14
[20] *See* The Connected World: Examining the Internet of Things: *Hearing Before the Senate Comm. on Commerce Sci. and Transp.*, 114th Cong 94 (2015).
[21] *Id.*
[22] *See* FPF, *supra* note 16, at 4.
[23] *See* Karkazis, *supra* note 9, at 20-21 (explaining that it is unclear whether HIPAA applies to biometrics collected outside of medical examinations because the data is not necessarily PHI and because organizations in professional sports may not be "covered entities" for this purpose.); *See also* Jessica L. Roberts et. al., *Evaluating NFL Player Health and Performance: Legal and Ethical Issues*, 65 U. PA. L. REV. 227, 265 (2017) (stating that the ADA only applies if a device is deemed "medical." It is unclear whether wearables meet this standard because they do not require the expertise of a healthcare professional, do not need to be used in a medical setting and are not obviously medical equipment specifically designed to detect impairment.).

Additional new approaches to data protection have sought to classify user information by "sensitivity" in order to apply FIPPs.[24] The Future of Privacy Forum (FPF) discusses this framework in its "Best Practices for Consumer Wearables &Wellness Apps & Devices."[25] The FPF urges collectors to separate user data into "sensitive health" data and "non-sensitive lifestyle" data and, from there, calibrate privacy protections and legal frameworks to the specific nature of the data collected.[26] "Where personal health or wellness data are inherently more sensitive . . . their collection and use should be . . . narrower . . . [requiring consent] for each specified use; and all advertising should be based on express consent."[27] By contrast, collecting "lifestyle data," like steps taken or calories burned, should not require individualized notices for "each and every compatible collection or use."[28] Instead, notice of a general purpose should "appropriately capture a range of tightly related purposes and advertising should be presented on an opt-out basis."[29]

III. Analysis

In 2016 the National Football League Player's Association (NFLPA) stated that "[t]eams should have policies in place that ensure the confidentiality, privacy, and security of any and all data/information collected via sensor devices."[30] To that end, the NFLPA articulated several "best practices" for the use of sensory technology in professional sports as a whole.[31] An

---

24 *See* FPF, *supra* note 15
[25] *Id.* at 2
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.* at 2-3
[30] Sean Sansiveri & Sophie Gage, *Important Considerations for Athletes in the Boom of Wearable Sensor Technology*, WORLD FED'N OF THE SPORTING GOODS INDUSTRY MAG., 2016, at 10, http://www.globalsportsjobs.com/article/important-considerations-for-athletes-int-he-boom-of-wearable-sensor-technology/.
[31] *Id.*

examination of these practices yields, essentially, the use of "targeted FIPPs." For example, the NFLPA advises:

> Data ownership, limitations on the use, sale and/or dissemination of the data, and provisions regarding the security and storage of the data, are all considerations that should be specifically addressed by contract.[32]

Yet, while the guidelines urge organizations to consider use limitations, they do not address specific mechanisms, contractual or otherwise, for doing so. The simple question remains, what, if any, degree of protection can players actually expect with regard to their data?

A. Health Data: The Highest Level of Protection

Article 51 Section 13(c) of the NFL Collective Bargaining agreement reads:

> The NFL may require all NFL players to wear . . . equipment that contains sensors or other nonobtrusive tracking devices for purposes of collecting information regarding . . . performances . . . and movements, as well as medical and other player safety-related data . . . Before using sensors for health or medical purposes, the NFL shall obtain the NFLPA's consent.[33]

In requiring consent for technology used "for health or medical purposes," the language of the CBA seems to fit the mold created by the FPF Best Practices to protect "more sensitive" data. Where an organization decides to utilize a device collecting "health" data, it must inform athletes of the purpose for collection and the intended use of the data. Organizations must then employ heightened levels of protection, and, most importantly, retain a specific level of consent. This ensures that use is narrowly tailored to the objective of ensuring the health of the player and providing the best possible care if need be. Absent such protections, players can only trust that "[their] employer will analyze only what [they are asked] to detect."[34] Many doubt that

[32] *Id.*
[33] 2011 NAT'L FOOTBALL LEAGUE COLLECTIVE BARGAINING AGREEMENT art. 51 (Aug. 4, 2011).
[34] Pablo S. Torre & Tom Haberstroh, New biometric tests invade the NBA, ESPN (Oct. 10, 2015), http://www.espn.com/nba/story/_/id/11629773/new-nba-biometric-testing-less-michael-lewis-more-george-orwell.

organizations will be able to resist temptations to engage in unexpected uses without a form of heightened security.

B. Performance Data: The sports equivalent of "lifestyle" data

There is, however, a wide array of data falling outside the more sensitive medical context. For decades teams have used "performance" indicators like speed, strength, and agility to evaluate their athletes. While in some instances this might mean using a stopwatch, in others it could mean monitoring millions of data points through Catapult Optimeye GPS tracking technology.[35] Few would argue that a player's 40-yard dash time should be subject to the same forms of heightened protection as his health information, but why should the principle change just because more advanced technology allows for better metrics? After all, "performance" data seems to fall within the scope of "low-impact" "lifestyle data" as described by the FPF.[36] Players should not expect lifestyle data to be afforded the same heightened protections as "health" data because lifestyle data does not expose private health information or enable conclusions to be drawn as to health status.[37]

The less sensitive treatment of performance data does not sit well with players. As Adam Warren of the New York Yankees explains, "if you're not the greatest at a certain [metric], does that affect your contract? Does that affect how the team sees you?"[38] The short answer is yes, but this stance is not as harsh as it might seem. Consider the following example: in 2014, ESPN linked declining performance in NFL running backs with reaching the age of twenty-seven.[39] "Decision-makers . . . saw that trend as a bad investment. As with any business, [teams] reserve

[35] *Outdoor,* Catapult USA (2017), http://www.catapultsports.com/system/outdoor/.
[36] FPF, *supra* note 15, at 2.
[37] *Id.*
[38] Lemerie, *supra* note 12
[39] Kevin Seifert, Inside Slant: Running back cliff after age 27, ESPN (2014), http://www.espn.com/blog/nflnation/post/_/id/123542/inside-slant-running-back-cliff-after-age-27.

premium contracts for projected growth in production, not a decline."[40] Coincidently, twenty-seven is when most NFL players become eligible for free agency.[41] As a result, when it comes time to make evaluations or financial commitments, teams give signs of declining production greater weight. The outcome should be no different simply because a team chooses to use a more revealing form of performance evaluation. If teams know decline is inevitable and are already hesitant to make a long-term investment, more advanced metrics do nothing more than confirm such suspicions. But what of the player who shows no decline at this stage? Here the advantage of better metrics multiplies. With tools like Optimeye, organizations are better equipped to assess the performance of this player objectively based on data, instead of assuming it is only a matter of time until performance declines. The benefits, therefore, break in both directions.

One aspect that organizations and their players can agree on is that there are dangers in sharing this data outside the organization without heightened authorization. It is again useful to think in terms of reasonably expected use.[42] This is especially important where a third party collects and analyzes player data on behalf of an organization.[43] On one hand, a player might expect the third party to share his running speed with coaches or trainers. However, an athlete certainly would not expect a collector to share such data with the general public and permit it to "test their speed" against the athlete's in an advertising gimmick. Moreover, unauthorized disclosure of performance data could be misused in contexts such as gambling and fantasy sports.[44] As the de facto proprietor of player data in the performance context, it is most

[40] *Id.*
[41] *Id.*
[42] See FTC Report, *supra* note 14.
[43] See Karkazis, *supra* note 9, at 54
[44] Marc Tracy, With Wearable Tech Deals, New Player Data Is Up for Grabs, New York Times (2016), http://www.nytimes.com/2016/09/11/sports/ncaafootball/wearable-technology-nike-privacy-college-football.html.

appropriate and a best practice for teams to give players the opportunity to "opt-in" to specific promotional or otherwise non-performance uses of this data.

C. Combating Grey Areas: Intended Use and Reasonable Expectations

The physical nature of sports suggests that some measurable data may fall within the scope of "performance data," but also qualify as "health data." Different uses could subject the data to very different expectations of privacy. Concussion detection presents an opportunity to examine this issue in more detail.

Obviously, analyzing "hits to the head" has relevance in the medical context. However, on the performance side, concussions have an equally strong link to diminished ability and production.[45] It is almost impossible to consider one aspect without the other. Can organizations allow the use of this data to indicate when players should be removed from games or treated for head injuries, but not allow the same data to influence a player's value? In reality, whether a team measures impact data using wearable sensors, or simply counts "blows to the head" on a pad of paper, a negative result still renders the player a "high risk." It should not matter whether information is "health related" or seemingly more sensitive in this particular context. If organizations can present a clear, statistically proven link to performance, they should have discretion over how much weight to give a certain metric. Ultimately, nothing can stop players from rebutting the data at the negotiating table, but they should not expect to control its use to their detriment.

An additional concern is that goals "can easily slide from improving performance to . . . making sure [players] don't do anything to embarrass the team . . ."[46] For example, while a

[45] *See* Cynthia W. Majerske et. al., *Concussion in Sports: Postconcussive Activity Levels, Symptoms, and Neurocognitive Performance*, 43 J OF ATHLETIC TRAINING 265, 265-266 (2008).
[46] Torre, *supra* note 34

wearable "patch" might show that a player slept just three hours the night before a game, it might also indicate that his heart rate was consistent with intoxication.[47] Should organizations be able to use this "performance" information in a disciplinary context? Again, the answer depends on expectations. Where a player is notified that data will be collected for performance purposes, he expects it to be used to better his "game," not judge his life choices. While it is unlikely that a player will be able to stop the team from observing his off-time behaviors altogether, use of this information to the player's detriment, without a clear link to poor performance, should warrant additional privacy protections as a "non-performance use."

IV. Conclusion

The next steps in wearable technology and biometrics will revolutionize coaching, training, and player management, and "stream in" the next frontier of legal issues in professional sports. Given the lack of federal guidance in this arena, it is important to exchange ideas and develop a regulatory framework to ensure that the next steps are the right steps. Ultimately, both the athlete and the organization want to perform at the highest level, but that does not mean data collection should go unchecked. We need to discern from the ever-increasing pool of gatherable metrics which data is more sensitive and worthy of greater protection and authorization. This cannot be done without considering the purpose for collection and the athlete's reasonable expectations about the use of such data. While data collected with no clear link to performance may warrant greater levels of security, data directly tied to and collected for performance assessment should not come with an expectation of heightened protection.

[47] *See id.*