

Cybersecurity in Sports

Questions of Privacy and Ethics

Max Greenwald, Tufts University

December 2017

Abstract

With increasing frequency, organizational databases and medical devices are becoming network-connected and data driven so that doctors, researchers, and patients can benefit from accessible, reliable, and current health information. In sports medicine, this data exchange can be especially helpful for athletes in order to prevent injuries and improve athletic performance. However, security vulnerabilities and a lack of security regulation surrounding this data presents a risk to athletes and their personal privacy, as well as the market surrounding the game, including bets on game results, ticket sales, and advertising contracts. While real-time transfer of data during games and practices can allow for immediate diagnoses, there is a risk that transferred data can be stolen and used for criminal purposes. This article will explore previous data breaches of private athletic data, analyze the ethical concerns and security risks surrounding the use of big data in sports, and provide action items for sports organizations to improve their cybersecurity efforts.

Contents

1	Introduction	3
2	To The Community	4
3	A Case Analysis of Security Breaches	4
3.1	WADA Doping	5
3.2	Fitbit Wearables	6
3.3	Houston Astros Hack	6
4	Data in Sports	7
4.1	Big Data	7
4.2	Ethical Questions	8
5	Security of Devices Used in Sports	9
5.1	Big Security	9
5.2	Real Time and Future Targets	10
6	Action Items	11
7	Conclusion	12

1 Introduction

Widespread technology use in sports started with the integration of video cameras to record and later broadcast games instantly around the world. As broadcasting technology developed, teams and players began to use videos to learn about and improve athletic performance. Referees began using instant replays to ensure the validity of calls, and MLB broadcasts began showing the strike-zone on screen as if it existed in the real world. And now, in the 21st century, technology is being used in sports to do so much more.

Sports organizations have begun amassing data about individual athletes such as acceleration, heart rate, and sleep. This data is closer to the individual than ever before: while statistics in baseball like *Earned Run Average* and *On Base Percentage* have to do directly with game play, this new data functions as an electronic medical record and is intended to improve performance and decrease injuries. In addition, medical devices like sensors in football helmets that detect potential concussions can not only prevent injuries but also save lives.

The explosion of big data in the past decade has sparked a debate over the ethics of sharing the private information of public figures such as professional athletes. Athletes are now subject to decreasing privacy in the media and increased monitoring by their organization or team, and as such can be treated as commodities instead of employees [11]. While some athletes are comfortable with this kind of monitoring, sports organizations do not always clearly communicate to their athletes the extent to which they monitor and share data on individual athletes [4].

As devices and data become more prevalent and useful, the security of these devices and the storage of the associated data is essential for the privacy and safety of athletes and the success of sports organizations. While more data is becoming available, it is important to continue to audit data systems, monitor for potential breaches, and inform all parties, especially the athletes, about their rights and responsibilities surrounding the use and distribution of their data. The use of these technologies presents great benefits, but alongside them arrive risks and responsibilities.

2 To The Community

Sports and sports medicine are topics that are important to me. I grew up in a family of sports lovers, players, and researchers. Both of my parents studied sports medicine, and now my Dad runs a company called Simbex (Simply Better Exercise) that makes sports medical devices and my mom is a personal trainer. I have played sports for my whole life, and throughout my middle school and high school sports career I saw positive changes in safety and tactics that came from big data and research such as decreased hitting practices in football and weaker aluminum and compound bats in Little League Baseball. While the privacy debate discussed in this article focuses on professional sports, the advances in game-play tactics and player safety that are made in professional sports also affect 45 million children in the United States who play sports each year [1].

Security in sports has implications for everyone, not just the athletes and employees involved in professional sports. While the data coming from new technologies can improve sports performance, the privacy and security concerns that come with storing and transmitting this data have not been fully addressed by the community through regulations and standards. Public releases of sensitive data by hackers has the potential to impact the lives of athletes, members of the organization, and markets surrounding ticket sales and sports betting. As smart watches and other wearables increase in popularity, the growing quantity of individual employee data that large corporations store will increase drastically. Thus, the ethics debate over the privacy of professional athletes will inform the same debate for employees in the workforce.

3 A Case Analysis of Security Breaches

While some Cybersecurity research flirts with the sexiest new hacks, the most devastating hacks usually come from easily fixable flaws or mistakes. In this section, we will explore three real-world cybersecurity breaches and threats in athletics.

3.1 WADA Doping

In September of 2014, the New York Times published a story about a hack of the World Anti-Doping Agency (WADA), allegedly by the Russian cyber-espionage group Fancy Bear. Fancy Bear released private medical information and evidence of doping on 41 Olympic athletes, including three famous United States athletes: Tennis players Serena and Venus Williams and Olympic gymnast Simone Biles. Even though each of the United States athletes tested positive for using banned substances, they all had received the proper permission to do so from WADA.

The attack on WADA was a spearphishing attack, a method of Social Engineering. Spearphishing is very difficult to protect against as it does not exploit flaws in code, but instead takes advantage of real people. In a spearphishing attack, emails that look real and important but instead contain malicious links are sent to known targets by attackers. The links go to websites that look like real websites that prompt users to enter real credentials that are then stolen. These attacks can be devastating because they target the people who are least expecting it instead of those who are working to protect and secure user data.

While the specifics of the WADA spearphishing attack are confidential, a typical spearphishing attack might go like this:

- An unsuspecting user receives an email that looks legitimate
- The user clicks on a link in the email and enters their credentials on the webpage
- The webpage has unexpected behavior, but does not in fact log the user in. The web page is malicious and stores the user's credentials to the real website
- Attackers use the credentials to log in to the real website and steal user data

The best protection against this kind of attack is education about phishing attacks. Knowing what phishing emails look like can help prevent these attacks from happening.

The WADA attack targeted WADA employees and was a potential retaliation against investigations into Russian doping in the 2016 Olympic games in Sochi. The data released contained private information about athletes, and is detrimental to the public trust in WADA and also Russia [10].

3.2 Fitbit Wearables

Wearables, which are becoming the standard in sports to track biometric data, are not without their own security flaws. While a large breach of data from a wearable device or a wearable device company has yet to be disclosed publically, security researchers have demonstrated flaws in some wearable products, like the wearable watch Fitbit, which tracks biometric data such as location, heart rate, and number of steps. In 2015, a researcher at the security company Fortinet posted a video demonstrating that malicious code could be injected onto a Fitbit device [13]. And, in September of 2017, a research team from the University of Edinburgh demonstrated at the security conference RAID that they could, using a modified Fitbit watch, access and change user data on the server. Fitbit has since patched this latest security vulnerability [7], but security on smartwatches like these are still weak .

A potential reason for a lack of security for wearables is that policy and law for wearables and other Internet of Things (IoT) devices has lagged behind security standards for desktop computers. For example, policies put out by the IBM company Fiberlink called "Mobile Device Management (MDM) Policies" still do not cover best practices for wearable and other IoT devices. If policies are not up to date, emerging companies may not use best practices. This could allow hackers to use techniques like bluetooth sniffing to detect local wearable devices and collect sensitive data if the information being sent over the network is not encrypted [2]. In order to prevent against these kinds of attacks, developers must be aware to use encryption when sending sensitive data, and also to encrypt any passwords or other information that is temporarily stored on the device. For sports organizations, prevention efforts should include proper research into the security practices of the wearable device company and internal education and preparation on what could happen if sensitive data is leaked.

3.3 Houston Astros Hack

Employees of the St. Louis Cardinals broke into the Houston Astros' computer network in 2013. The employees used an old password of the former Cardinals general manager and current Astros general manager Jeff Luhnow to break in. The Astros database included player data, internal trade discussions, and other proprietary information regarding team statistics. While the F.B.I. has not disclosed the severity of the breach, the break-in was not

discovered for a number of months, so it is possible that all of the data in the system was stolen.

This kind of attack is not necessarily commonplace, but it is definitely the easiest and most important attack to defend against. When the Houston Astros set out to build a database of player data, they modeled it off of the Cardinals system due to Jeff Luhnow's experience with the Cardinals. The striking similarities between the two systems, including Jeff Luhnow's identical credentials, made it particularly easy for Cardinals employees to log in using a master list of Luhnow's passwords [12].

In order to defend against this, the Astros should have engaged in security audits. A security audit is a check on the security of internal systems, usually by an outside party or organization, in order to find potential flaws. An audit would have most likely found out that Mr. Luhnow used passwords similar to previously used passwords, or implemented a policy where passwords are changed after a certain amount of time.

4 Data in Sports

Recent technological advances in sensors, storage capacity, and computing have produced a huge amount of data about athletes. Sports franchises are now storing and using this data for research in order to win more games and bring more customers to the stadiums, thus increasing profits. However, with big data can come even bigger security problems and ethical questions about player privacy.

4.1 Big Data

Professional sports leagues are moving towards tracking and storing more player information than ever before. In April of 2017, the NFL Players Association (NFLPA) released details of a five-year deal with the wearable company WHOOP. The partnership will allow NFL players to track their own health using statistics like sleep, exercise, and recovery. In addition, the NFL currently partners with Zebra Technologies in order to track players on the field during games while the MLB approved the use of WHOOP during games in March of 2017. The NFL and the NBA currently bar the use of such wearables in-game, preferring their own player tracking technology. [14]. The NFL shares player movement data with each team, but excludes data

from other teams [6]. The MLS in 2012 began using Adidas' Micoach Elite System technology, which sends heart-rate, movement, and other health data in real-time to mobile devices in real-time [9].

This player data is used in a variety of ways: athletes use their own data to improve their sleep, eating, and workout routines; coaches use the data to analyze games, tactics, and individual performances; personal trainers use the data to diagnose injuries or disease preemptively; and leagues and oversight organizations use the data to develop new rules to improve safety and attract bigger crowds. There are huge benefits to using this data, and machine-learning and real-time analytics have only recently started gaining traction.

4.2 Ethical Questions

This wave of big data also comes with big questions. Who owns the data? How is the data stored? Can this data be sold for a profit? How should the data be transmitted? Can a team use this data against a player's contract or in contract negotiations? Currently there are very few regulations on data use, other than laws that aim to prevent disability and genetic discrimination against employees or players. The big data currently belongs to the teams that generate and use the data, but there is no regulation on how this data should be stored [3].

Athlete privacy is also central to this debate. Is it breaching a player's privacy to continuously monitor their activities wherever they go? While an athlete certainly has the right to choose not to work for an organization that wants to monitor him or her around the clock, the choice to find work elsewhere is not usually readily available. Thus, organizations must consider the strain they are putting on athletes by requiring such full-time monitoring. Any such monitoring should be fully endorsed by the athlete as a way to improve and learn more about themselves. Athletes should be able to trust institutions with their data. However, this trust has been broken in the past: genetic data tests on athletes may be given to WADA, an organization that was previously hacked. Leaked genetic data could expose private information about the relatives of an athlete who share a very similar genome [8].

There also arise large ethical questions about medical treatment in relation to the data that IoT devices give us. Even though new technologies can provide athletes with great medical treatment, the lack of long-term medical studies surrounding this new information can lead to improper treatment.

In addition, allowed performance-enhancing drug use is a gray area for many sports doctors as it can be unclear whom the doctor is loyal to: the team, the athlete, or a regulatory body. Doctors must abide by the HIPAA law regarding patient confidentiality, but also are pulled in many directions by the abundance of data available to them and the wills of all parties involved. Athletes do not always know the extent or severity of their treatment, and it is up to the doctor to explain to the patient the best treatment methods while also balancing data about the patient from medical devices that are not necessarily trustworthy [3].

Currently, there is no governance framework over the use of data in sports. In a 2016 paper titled "Ethics, Nanobiosensors and Elite Sport: The Need for a New Governance Framework", Evans et al. conclude that there is a need for a governance framework:

"Before Nanobiosensors become an everyday tool of sporting performance analysis and enhancement, considerations of their dis-benefits—in terms of data access, ownership, confidentiality, privacy, and also athlete welfare, must be taken into account by sporting regulatory bodies to consider the impact they may have not only on the athlete, but also the sporting system."

Governance bodies could be put in place to protect the interests of athletes as well as organizations. However, it is important to ensure that these bodies do not fall under duress from big donors and the parties that they are purportedly protecting [4].

5 Security of Devices Used in Sports

5.1 Big Security

With all of the data being stored, there is accompanying security risk. That risk begins the second the data is recorded or stored onto any device. If the device is a wireless IoT device or a Bluetooth-connected device, there is an inherent security risk as the data must be transmitted over a wireless connection to a database. If this data is not encrypted as it is sent, attackers can easily steal the data through network sniffing. Once the data is stored into a database, improper user permissions could lead to unauthorized access. All users must be authenticated through a rigorous process to access the data,

and all access should be logged. Passwords should be changed frequently, and the database should ideally be kept behind a firewall or private network in order to ensure that no outside or unwanted access is possible.

With the North American sports market projected to reach \$73.5 billion in 2019, there is a lot of money at stake for athletes, teams, and leagues as they attempt to increase their profitability [5]. The NFLPA deal described above even has the potential to make money for players as their data sets are sold for external use [14]. In addition, Olympic competitions bring an influx of people and money to a country and city in preparation for the Olympic events and during the actual competitions. Although it is very difficult to estimate the cost of a *generic* security breach for teams and organizations, any breach of data surrounding one of these organizations would involve a huge cost for an investigation, fixing the security flaw, and dealing the the consequences of leaked data.

5.2 Real Time and Future Targets

Currently, wearables and other IoT devices are potentially easy targets as they are usually internet connected and contain little on-device storage, and thus must transmit their data immediately over the internet. Additionally, team and organizational databases are targeted as they contain large amounts of athlete data in one place. A great example of this is the WADA hack, as information about athletes from multiple sports was released to the public, and it is very possible that attackers accessed the entirety of the entire WADA database in the process.

In the future, it is possible that hackers may attempt to hack refereeing equipment in order to either change the results of a contest or point blame at another organization or country. Also, teams could intentionally tamper with their own data to make it look like they are following league rules. Athletes could tamper with their own metrics to affect future contract offers, and could also work to sabotage the data of other athletes to gain a competitive edge. And, when the flood gates to genomic testing are opened, a data breach could cause the leakage of genetic codes of athletes across the internet for malicious use.

6 Action Items

These action items are intended for sports organizations or security professionals working for those organizations in order to improve security standards and increase security awareness.

- **Perform routine security audits**

Routine security audits entail hiring a professional security organization to audit the security of all technology being used. For a sports organization, this could mean an audit of all internal databases, user systems, and devices that communicate with one another and store sensitive data. An audit might determine that coaches are using insecure passwords, such as in the Houston Astros hack, or could find an open database that could be accessed by anyone without authentication.

- **Educate athletes, coaches, employees on information security**

In order to protect users from scams such as phishing and to encourage users on good security practices like strong passwords, education is essential. There are many resources available online about IT education.

- **Hire a dedicated security professional**

While a software engineer is a good first step to providing good security, a dedicated security professional can work full time to detect and protect against threats that a software engineer does not have knowledge about or does not have time to think about.

- **Take data offline whenever possible**

The easiest solution to data breaches is to remove sensitive data from any internet-connected devices. While this may remove some ease of use, it is the best way to protect sensitive data. Only allowing access to sensitive data in-person is a great way to verify the real identity of users accessing data.

- **Don't sell data**

Selling any data, even de-identified data, could lead to data being exposed externally in ways that cannot be internally monitored. De-identified data can sometimes be re-identified based on the contents of the records.

- **Advocate for regulatory bodies to protect athletes and sports organizations**

The best way to ensure that all sports organizations and athletes are protected is to advocate for governance bodies that create best practices and disseminate new information throughout the sports community. Without these regulatory bodies, there is no hope for consistency in threat detection, protection, and response between different organizations.

7 Conclusion

The cybersecurity issues facing athletes and sports organizations has the potential to pose great risks to the privacy and security of the lives of athletes and can impact the earnings of these organizations as well as the public trust in professional sports institutions. As wearable devices become ever more present and big data becomes increasingly vital to the success of athletes, security flaws pose a threat to the fundamental privacy of people. It is ever more important to be cognizant of these issues and to bring people together in combating cybersecurity threats. Sports will continue to use more and more technology, and this is important and good: it will continue to advance competition in terms of safety and performance. However, we must not take these technologies or the privacy of individuals for granted, and must strive for consistency and best practices within its future use.

References

- [1] Jay Atkinson. *How parents are ruining youth sports - The Boston Globe*. May 2014. URL: <https://www.bostonglobe.com/magazine/2014/05/03/how-parents-are-ruining-youth-sports/vbRln8qYXkrrNFJcsuvNyM/story.html>.
- [2] Samantha Donaldson. *Wearable Tech: A Developer's Security Nightmare*. Mar. 2017. URL: <https://developers.redhat.com/blog/2017/03/06/wearable-tech-a-developers-security-nightmare/>.
- [3] Warren R. Dunn et al. "Ethics in sports medicine". In: *The American Journal of Sports Medicine* 35.5 (May 2007), pp. 840+. ISSN: 03635465. URL: http://link.galegroup.com/apps/doc/A165764780/AONE?u=mlyn_m_tufts&sid=AONE&xid=08de267f.
- [4] Robert Evans, Michael McNamee, and Owen Guy. "Ethics, Nanobiosensors and Elite Sport: The Need for a New Governance Framework". In: *Science and Engineering Ethics* 23.6 (2017), pp. 1487–1505. ISSN: 1471-5546. DOI: 10.1007/s11948-016-9855-1. URL: <https://doi.org/10.1007/s11948-016-9855-1>.
- [5] Darren Heitner. *Sports Industry To Reach \$73.5 Billion By 2019*. Mar. 2016. URL: <https://www.forbes.com/sites/darrenheitner/2015/10/19/sports-industry-to-reach-73-5-billion-by-2019/#6e19210f1b4b>.
- [6] Daniel Kaplan. *NFL slows sharing of player tracking data*. Aug. 2016. URL: <http://www.sportsbusinessdaily.com/Journal/Issues/2016/08/01/Leagues-and-Governing-Bodies/NFL-data.aspx>.
- [7] Cara McGoogan. *Fitbit devices can be hacked, research shows*. Sept. 2017. URL: <http://www.telegraph.co.uk/technology/2017/09/14/fitbit-devices-can-hacked-research-shows/>.
- [8] Michael John McNamee et al. "Genetic Testing and Sports Medicine Ethics". In: *Sports Medicine* 39.5 (2009), pp. 339–344. ISSN: 01121642. URL: <http://search.ebscohost.com/login.aspx?direct=true&db=s3h&AN=43531448&site=ehost-live>.

- [9] Raju Mudhar. *New technology turning athletes' bodies into open book: Mudhar*. July 2012. URL: https://www.thestar.com/sports/soccer/2012/07/23/new_technology_turning_athletes_bodies_into_open_book_mudhar.html.
- [10] Rebecca R. Ruiz. *Simone Biles and Williams Sisters Latest Target of Russian Hackers*. Sept. 2016. URL: https://www.nytimes.com/2016/09/14/sports/simone-biles-serena-venus-williams-russian-hackers-doping.html?_r=0.
- [11] Jimmy Sanderson. "Professional Athletes' Shrinking Privacy Boundaries: Fans, Information and Communication Technologies, and Athlete Monitoring". In: *International Journal of Sport Communication* 2.2 (2009), pp. 240–256. ISSN: 19363915. URL: <http://search.ebscohost.com/login.aspx?direct=true&db=s3h&AN=40731766&site=ehost-live>.
- [12] Michael S. Schmidt. *Cardinals Investigated for Hacking Into Astros' Database*. June 2015. URL: <https://www.nytimes.com/2015/06/17/sports/baseball/st-louis-cardinals-hack-astros-fbi.html?smid=tw-bna>.
- [13] Chris Smith. *Hackers can invade a PC with a 10-second attack on a Fitbit*. Oct. 2015. URL: <http://bgr.com/2015/10/21/fitbit-malware-hack-pc/>.
- [14] Tom Taylor. *Football's Next Frontier: The Battle Over Big Data*. June 2017. URL: <https://www.si.com/2017/06/27/nfl-football-next-frontier-battle-big-data-whoop-nflpa>.