ATHLETE AND CONSUMER DATA PRIVACY CONCERNS

A Research Paper submitted to the Department of Engineering and Society
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Systems Engineering

By

Daniel Ungerleider

March 27, 2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISOR
Catherine D. Baritaud, Department of Engineering and Society

Sports analytics is becoming increasingly crucial to create competitive advantages in high-level athletics. At the University of Virginia (U.Va.), there are minimal opportunities for students to engage in sports analytics and the varsity athletics teams are inconsistent in their methods and volume of data collection and analysis. To resolve these issues, as well as to become a nationwide leader in sports analytics and to support U.Va. President Jim Ryan's 2030 strategic plan to make U.Va. both "great and good," the technical project recommends the design of a sports and performance analytics center at U.Va. (Hester, 2019, p. 1). This recommendation includes the physical location of the center, the logistics of data collection, storage, and analysis for all varsity teams, new opportunities for research in sports analytics as well as analytics in general, more expansive community outreach programs, and new educational opportunities within the subject areas of sports and performance analytics. As data collection from wearables and other technologies continues to increase, there are many ethical issues that arise creating conflict between the many actors involved and putting the relevant ethical values at risk. Tightly coupled with the technical project, the Science, Technology, and Society (STS) research paper examines the ethical concerns associated with data privacy as well as the status of current legislation existing to protect athletes and consumers alike. This includes the examination of new legislation which will affect student athletes and consumers nationwide (Stoltz, 2019). The Social Construction of Technology framework, adapted from Bijker and Pinch by W.B. Carlson (2009), is used to analyze and visualize the relationships between the many stakeholders involved in the context of data privacy for student athletes as well as consumers vulnerable to high levels of data collection. The technical and STS projects are tightly coupled; the STS research builds upon privacy issues briefly touched on in the technical project and generalizes many ethical issues associated with data privacy for all consumers.

CURRENT INCREASE IN DATA COLLECTION

The market for wearable technologies continues to skyrocket as the years go by; it is estimated by researchers Jason Arnold and Robert Sade that over 400 million wearable smart devices worth $34 billion will be sold in 2020. Of these wearable technology devices, approximately 60% are sports and fitness trackers (2017, p. 67). Accompanying the increased number of wearables is a large increase in the amount of data collected on each consumer. Sports and fitness trackers serve many purposes, all of which involve high levels of data collection using different methods including heart rate monitors, sleep trackers, accelerometers, GPS location sensors, etc. Universities around the country have become wide-ranging consumers of wearable technologies. Many teams believe in collecting and analyzing data on their student athletes which can lead to competitive advantages. The main users of data collected from wearables in collegiate athletics are coaches, trainers, and analysts, most of whom use the wearables for multiple purposes. Coaches and trainers use analysis from training sessions to improve training regimens; they also use data to adjust in-game decision making with the hopes of improving team performance in competition. In addition to data collected from wearables, many teams also collect information self-reported from athletes to promote injury prevention and positive nutrition habits. Self-reported data can include hours of sleep per night, food eaten each day, player readiness or injury status, as well as many others that can vary from team to team or school to school.

As the use of new wearables continues to skyrocket, big data technologies continue to arrive in the marketplace. When new big data technologies are implemented, there are many ethical and societal implications affecting consumers. La Fors, Custers, and Keymolen, who are Dutch professors of ethics and law in relation to data protection, big data, and new technologies,

argued that many complications arise in adhering to widely accepted moral values when implementing new technologies. La Fors et al. compare the implications of big data technologies to those of the Industrial Revolution (2019, p. 212).

DATA PRIVACY CONCERNS

Currently, there is a lack of regulation existing to protect the data privacy of student athletes and consumers. Student athletes do not have much control over how data is used for or against them. According to Wake Forest School of Law graduate Gilbert Smolenski (2019), college teams that track player health and sleep data can punish athletes for not getting enough sleep or for having poor nutrition (p. 296). Furthermore, conclusions obtained from training and performance data can reveal that certain athletes are not as effective in their sport as previously believed, possibly leading to less participation in competition and a worse experience for many athletes. Athletes do not have much say over what data is or is not collected on them or how it used for or against them. Researchers Jason Arnold and Robert Sade (2016) admitted "federal regulations do not address the use of biometric technologies in [college] sports" (p. 70).

Figure 1, shown on page 4, is a Technology and Social Relationships diagram, a specific application of the Social Construction of Technology adapted from Bijker and Pinch by W.B. Carlson (2009). Trainers and analysts are at the center of the framework as they are the actual users of the data obtained from wearable technologies worn by athletes. They analyze the collected data to create valuable insight for their respective teams. As previously explained, the users of the technology have goals to improve individual and team performance as a result of conclusions obtained from data analysis. Coaches then use these conclusions to make decisions for training and competition plans; they hope the data will provide competitive advantages for

performance. Seen in Figure 1 below, there is an arrow connecting the coaches with the athletes; this is because athletes are directly impacted by the results found by the trainers or analysts and used by the coaches. Athletes do not have control over the analysis that is done or the team decisions that are made following the findings. This is not ideal for athletes since they are the ones who are actually wearing the technology in the first place, but they do not have any power in this framework. The other stakeholders involved are the engineers and the regulators. The engineers, who design the wearables and are responsible for the extent of functionality the wearables have, do not necessarily have the athletes' or coaches' interests in mind, which is why they are somewhat isolated in this figure. The regulators are isolated as their purpose is to protect the user privacy, but they do not have relationships with other stakeholders.

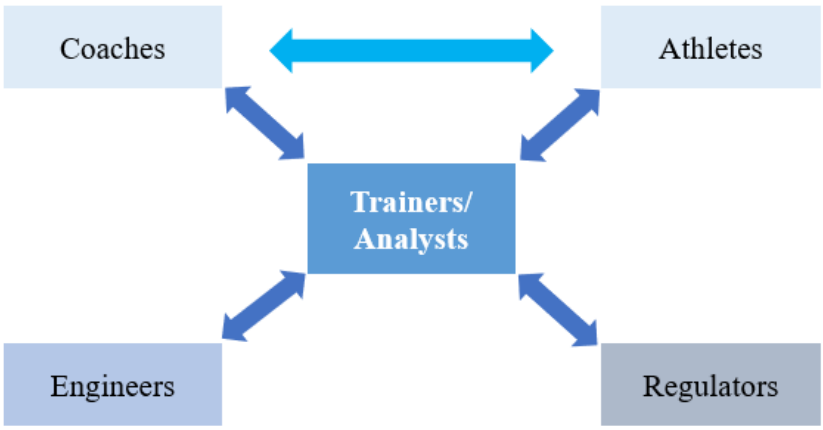

Figure 1: Technology and social relationships: A framework displaying the relationships involved in wearables within the context of collegiate athletics (Adapted by Daniel Ungerleider (2020) from W.B. Carlson, 2009).

Further putting athletes' data at risk, collegiate athletics organizations often do not store their data in a protected environment and current regulations are not sufficient in addressing this issue. Many teams do their analyses in-house, in which case trainers or analysts import data onto their personal laptops and do their analyses privately. This storage technique has caused issues in

the past at U.Va. in which the up-to-date analytics are lost as a result of a coach or trainer getting fired or quitting. The respective team then loses the current analytics results; they also have no control over what the former trainer or analyst does with the data they have taken with them.

With regard to all consumers, companies now collect vast amounts of consumers' personal data without revealing the extent of data collected or how it is used. Often times consumers have no idea what information is even being collected. Companies generally have user privacy agreements consumers have to sign, but they are outrageously long and it is not realistic to expect consumers to actually read them. Wearable technology companies have little incentive to focus on protecting consumer's data privacy because there are little to no consequences these companies are responsible for. The Health Insurance Portability and Accountability Act (HIPAA), which was signed into law in 1996, was originally enacted to keep patients' medical records safe, but to also serve as protection for consumers' personal and health data. However, it has limitations, and according to data privacy expert Gicel Tomimbang (2018), "Wearable devices fall outside federal regulatory frameworks" and "wearable device companies have limited [liability] exposure under HIPAA" (p. 3).

Figure 2, shown on page 6, reveals a Systems in Context diagram that examines the actors involved within the context of big data technology development and implementation. In the center of the diagram are the technology companies who are responsible for the development, implementation, and maintenance of big data technologies. They decide which factors are important to them and which ethical values they consider. On the boundary of technology development are the regulators; the level of regulation decides how careful the technology companies are in their development. On the outside of this boundary are the consumers of the technologies. The consumers do not have much power in this system; they are merely the end

users and are not involved in the development or implementation of new technologies but only in the use of them.

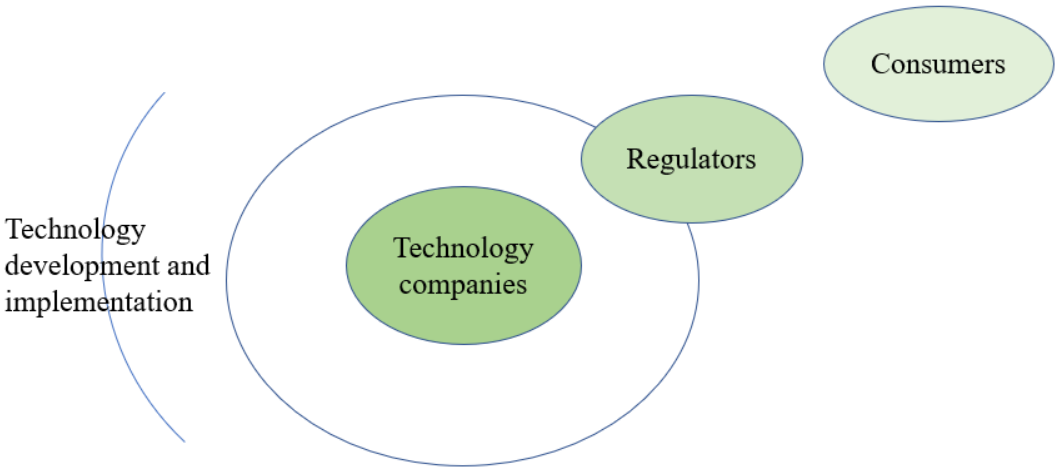

Figure 2: System in context: Framework within the context of big data technology development and implementation (Adapted by Daniel Ungerleider (2020) from W.B. Carlson, 2009).

When companies develop and implement big data technologies, the current approach for the majority of companies is not holistic enough; they do not integrate existing methods of using moral values for guidance. Instead, companies use isolated, individual moral values to help guide them in the development and implementation of new technologies. Oftentimes, the current approaches companies use regarding moral values lead to conflict and result in products that do not satisfy critical ethical values.

HOW TO BETTER PROTECT DATA PRIVACY

With all of the complications and different factors that come into play, how can athletes and consumers have better protection and control over the vast amounts of data collected on them? To examine this, recent data privacy laws aiming to give consumers more control over their data and how it is used must be looked at. Up to this point, current legislation has lacked effective enforcement. It is also necessary to understand all the relevant ethical and societal

challenges resulting from new big data technologies which come into play throughout the entire process of big data technology development and maintenance. With time, companies will need to reassess the relevant values associated with emerging big data technologies (La Fors, Custers, Keymolen, 2019, p. 210).

ENFORCEMENT OF NEW LEGISLATION

The California Consumer Protection Act (CCPA) went into effect in January, 2020 and is meant to give consumers more control over their data. The law allows consumers to request and delete personal data that companies have on them (Korolov, 2019, p. 1). Companies the CCPA affects fall under at least one of the following two descriptions: 1) companies that serve California residents and have at least $25 million in annual revenue, and 2) companies of any size that collect personal data on at least 50,000 people or obtain more than half of their revenue from the sale of personal data (2019, p. 1). Companies do not even have to be based in California to be affected. Since the criteria above is very broad and has strong implications stretching far outside of California, the law affects companies and consumers nationwide. According to technology expert Kashmir Hill (2020), "to get your personal data, you may have to give up more personal data" (p. 2). When a consumer attempts to obtain data on himself, the company involved often requires further identity verification before the request is approved. This has involved sending a government issued ID accompanied by a selfie photo of the consumer's face to ensure they are in fact the involved person. In other cases involving established companies, the verification step has involved logging into an account and confirming an email address or phone number to verify identity. Many consumers have expressed anger over having to provide additional information on themselves to obtain the data they requested. However, Hill expresses these extra steps are necessary to prevent fraudulent requests from successfully going through

(2020, p. 2). There have been many situations in which users have purposefully fooled the system and obtained personal data on other individuals, including mailing addresses, social security numbers, credit card information, etc., which should never have gotten into the fraudulent hands of the individual who requested the data. Hill expresses that companies need to "improve their security practices to avoid compromising customers' privacy further" (2020, p. 2).

In addition to compromised privacy, the enforcement of this new law as well as others similar to it has not been effective. Since the CCPA came into effect in January 2020, the enforcement of the law has not yet been sufficiently invested in and likely will not be until at least six months from the law going into effect. Since the law was passed in 2018, companies were supposed to have their data tracking systems in place by the beginning of 2019. However, human resources available for enforcement are not adequate, and potentially only up to three cases can be reviewed in a given year (Hill, 2020, p. 2). The lack of enforcement is significant since affected companies still do not fully understand how to abide by the new law. The law also allows consumers many opportunities to sue, so there will likely be many cases with a lot of money on the line. To effectively enforce the CCPA and other laws likely to follow, regulators will need to improve the current lack of resources available for this purpose as well as more explicitly express what is considered acceptable and not acceptable so companies can have more preventative steps in place during the process of data collection.

Other laws similar to the CCPA are very likely to be passed in the near future and to follow in this law's footsteps as it is very crucial to ensure data privacy and provide consumers with more control over their information. Data privacy researcher Tucker Partridge (2019) admits he expects states nationwide to follow California's lead on the CCPA and this type of

legislation has “been coming for a long time.” He expresses that giving consumers more power over data privacy is part of a “worldwide change in belief regarding data privacy” (p. 1). Additionally, he argues even though there is a political divide in the United States, bills improving the data privacy situation for consumers have begun passing and will continue to pass easily in the near future (p. 2). Companies must think more about the unintended consequences of empowering individuals with their personal data. Individuals need to understand that requiring identity verification when making requests for data control is meant to protect them and not harm them; these laws will continue to create conflict for the time being.

Figure 3, shown on page 10, displays many of the stakeholders relevant to new legislation involving data privacy and the implementation of new technologies. It is necessary to map the larger network of relevant stakeholders to better visualize who is involved as well as their role within the framework. Pacey’s Triangle provides a model to organize the major stakeholders into three spheres of influence: cultural, organizational, and technical (Pacey 1983). Many of the stakeholders inside of these branches could potentially overlap across multiple of the three options, but they are positioned in their best fit. The CCPA is already in effect and will impact other laws that follow, which is why it is located in the cultural section. The cultural section also contains consumer data privacy and other ethical values that must be considered; these are the driving forces behind new legislation and the need for better enforcement. The organizational section contains technology companies who are affected by new legislation and are also developing new technologies. It also contains legislators and regulators responsible for the improvement of the current situation. These groups must collectively commit to ensuring better data privacy and enforcement of new legislation. The technical branch contains consumer data and the wearable technologies involved. The ways in which the technical components are used

will be adjusted through new steps taken by the relevant organizations. It is clear that all three branches interact within the context of improving the current data privacy situation.

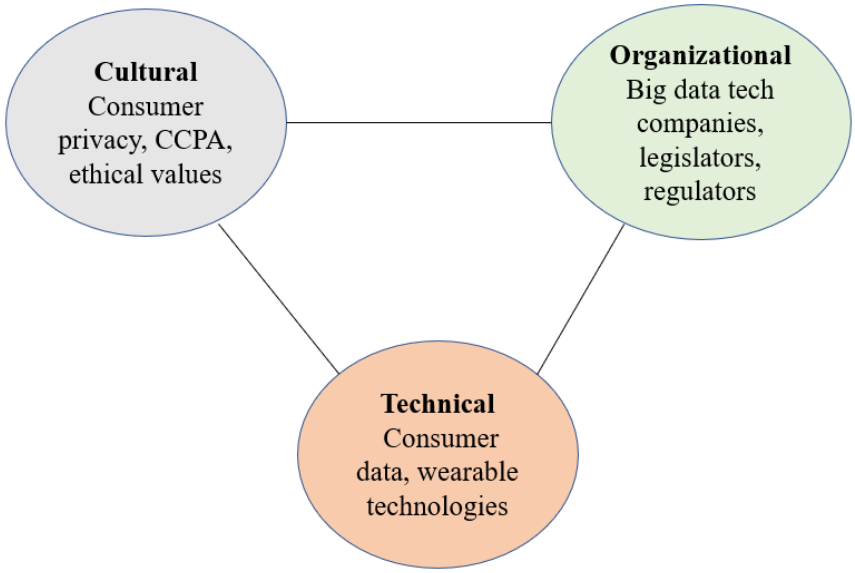

Figure 3: Data privacy legislation triangle: Stakeholders associated with new legislation in the context of data privacy (Adapted by Daniel Ungerleider (2020) from A. Pacey, 1983).

As new laws affect the practices of existing technology companies, many companies are continuing to implement new big data technologies. They must adjust their development approach when considering the ethical values of consumers. The current approach is not holistic enough and does not take into account sets of values instead of isolated individual values. There are two main current approaches to dealing with ethical complications in technologies: a design-based approach and an application-based approach (La Fors et al., 2019, p. 210). The design-based approach focuses on the ethical values relevant solely to the design of new technologies, whereas the application-based approach focuses on the ethical values relevant solely to how the new technologies will be used.

These approaches by themselves are not very acceptable because they lack the integration needed to consider sets of values at a time rather than individual values throughout the lifecycle of technology development, implementation, and acceptance. A more holistic approach involving the integration of existing methods results in a more accurate and adaptive network of actors affected by new technologies (Vedder and Custers, 2009, p. 22). Additional stakeholders, including policymakers and users, also have responsibilities of emphasizing relevant ethical values rather than being non-impactful bystanders. Looking at a more integrated approach has led La Fors et al. to create four main sets of moral values: techno-moral values, value-sensitive design, anticipatory emerging technology ethics, and biomedical ethics (La Fors et al., 2019, p. 223).

This integrative value approach to new technologies encourages companies to adapt and be more successful in ensuring data privacy and protecting consumers in the presence of big data technologies. Updated legislation meant to protect consumers and give them more control over their data is in the process of being developed and more effective enforcement will come with time. More resources need to be dedicated to improving the enforcement of new legislation. Technology companies must also do their part by taking preventative steps to improve data privacy and by creating more transparent privacy policies. As all of this is very context dependent, further research must be done to assess the fulfillment of necessary ethical values and the societal impacts of disruptive big data technologies.

WORKS CITED

Arnold, J., Sade, R. (2017). Wearable technologies in collegiate sports: The ethics of collecting biometric data from student-athletes. *American Journal of Bioethics, 17*(1), 67-70.

Hester, W. (2019, June 7). Ryan's "Great and good" strategic plan wins board endorsement. *UVAToday.* Retrieved from https://news.virginia.edu/content/

Hill, K. (2020, January 15). Want your personal data? Hand over more please. *The New York Times.* Retrieved from https://www.nytimes.com/

Korolov, M. (2019, October 4). California consumer privacy act (CCPA): What you need to know to be compliant. *CSO.* Retrieved from https://www.csoonline.com/

La Fors, K., Custers, B., Keymolen, E. (2019). Reassessing values for emerging big data technologies: Integrating design-based and application-based approaches. *Ethics and Information Technology, 21*(3), 209-226.

Partridge, T. (2019, October 8). Data privacy: How the current NCAA debate reflects the state of big data [Blog post]. Retrieved from https://www.zlti.com/blog/

Smolenski, G. (2019). When the collection of biometric and performance data goes too far. *Wake Forest Law Review, 54*(1), 279-301.

Stoltz, B. (2019, September 7). A new California privacy law could affect every U.S. business – Will you be ready? *Forbes.* Retrieved from https://www.forbes.com/sites/allbusiness/

Tomimbang, G. (2018, January 22). Wearables: Where do they fall within the regulatory landscape? *IAPP: The Privacy Advisory.* Retrieved from https://iapp.org/news/a/wearables-where-do-they-fall-within-the-regulatory-landscape/

Ungerleider, D. (2020). *Technology and social relationships.* [Figure 1]. *STS Research Paper: Athlete and Consumer Data Privacy Concerns* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Ungerleider, D. (2020). *System in context.* [Figure 2]. *STS Research Paper: Athlete and Consumer Data Privacy Concerns* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Ungerleider, D. (2020). *Data privacy legislation triangle.* [Figure 3]. *STS Research Paper: Athlete and Consumer Data Privacy Concerns* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Vedder, A., Custers, B. (2009). Whose responsibility is it anyway? Dealing with the consequences of new technologies. *Evaluating New Technologies,* 21-34.

BIBLIOGRAPHY

Arnold, J., Sade, R. (2017). Wearable technologies in collegiate sports: The ethics of collecting biometric data from student-athletes. *American Journal of Bioethics, 17*(1), 67-70.

Bloomfield, L. (2019). U.Va. class schedules: unofficial Lou's list: Obtained from U.Va. SIS. Charlottesville, VA. Retrieved from https://rabi.phys.virginia.edu/mySIS

Brown, S., Rasmussen, B. (2019, October 3). Personal interview [Interviewed by Sarah Nelson and Daniel Ungerleider]. University of Virginia. Charlottesville, VA.

Curtis, M. (2019, October 11). Personal Interview [Interviewed by Sarah Nelson and Daniel Ungerleider]. University of Virginia. Charlottesville, VA.

Hester, W. (2019, June 7). Ryan's "Great and good" strategic plan wins board endorsement. *UVAToday.* Retrieved from https://news.virginia.edu/content/

Hill, K. (2020, January 15). Want your personal data? Hand over more please. *The New York Times.* Retrieved from https://www.nytimes.com/

Korolov, M. (2019, October 4). California consumer privacy act (CCPA): What you need to know to be compliant. *CSO.* Retrieved from https://www.csoonline.com/

Kos, A., Milutinovic, V., Umek, A. (2019). Challenges in wireless communication for connected sensors and wearable devices used in sport biofeedback applications. *Future Generation Computer Systems, 92,* 582-592.

La Fors, K., Custers, B., Keymolen, E. (2019). Reassessing values for emerging big data technologies: Integrating design-based and application-based approaches. *Ethics and Information Technology, 21*(3), 209-226.

Martin, L. (2016). Sports performance, measurement and analytics: The science of assessing performance, predicting future outcomes, interpreting statistical models, and evaluating the market value of athletes. Old Tappan, NJ: Pearson Education, Inc.

Partridge, T. (2019, October 8). Data privacy: How the current NCAA debate reflects the state of big data [Blog post]. Retrieved from https://www.zlti.com/blog/

Reid, W. (2018, May 24). 'Hooball: The Cavalier football program is employing unique data models created by engineering students, some of whom are contemplating careers in the burgeoning field of sports analytics. *UVAToday.* Retrieved from https://news.virginia.edu/content/

Sharia, M. (2015, July 13). 5 amazing pieces of wearable tech being implemented in professional sports [Blog post]. Retrieved from https://www.wearables.com/blogs/news/

Smolenski, G. (2019). When the collection of biometric and performance data goes too far. *Wake Forest Law Review, 54*(1), 279-301.

Stoltz, B. (2019, September 7). A new California privacy law could affect every U.S. business – Will you be ready? *Forbes.* Retrieved from https://www.forbes.com/sites/allbusiness/

Swanson, S., Thomson, E. (2019, September 7). Personal interview [Interviewed by Sarah Nelson and Daniel Ungerleider]. University of Virginia. Charlottesville, VA.

Tomimbang, G. (2018, January 22). Wearables: Where do they fall within the regulatory landscape? *IAPP: The Privacy Advisory.* Retrieved from https://iapp.org/news/a/wearables-where-do-they-fall-within-the-regulatory-landscape/

Ungerleider, D. (2019). Gantt chart for capstone project. [Table 1]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Ungerleider, D. (2019). *Biofeedback system and loop operation.* [Figure 1]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Ungerleider, D. (2019). *Technology and social relationships diagram.* [Figure 2]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Ungerleider, D. (2019). *Cultural, organizational, and technical triangle.* [Figure 3]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Ungerleider, D. (2020). *Technology and social relationships.* [Figure 1]. *STS Research Paper: Athlete and Consumer Data Privacy Concerns* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Ungerleider, D. (2020). *System in context.* [Figure 2]. *STS Research Paper: Athlete and Consumer Data Privacy Concerns* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Ungerleider, D. (2020). *Data privacy legislation triangle.* [Figure 3]. *STS Research Paper: Athlete and Consumer Data Privacy Concerns* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Vedder, A., Custers, B. (2009). Whose responsibility is it anyway? Dealing with the consequences of new technologies. *Evaluating New Technologies,* 21-34.

Wasserman, E., Herzog, M., Collins, C., Norris, S., Marshall, S. (2018). Fundamentals of sports analytics. *Sports Medicine Statistics, Clinics in Sports Medicine, 37*(3), 387-400.