Biometrics Research Paper

ENG 211C- Drylie

Kris Vargas

The huge impact that technology has had on the world cannot be understated in any way. This can be seen in everyday tasks and activities, such as being able to facetime your friend that lives across the globe, having access to millions of movies on a handheld phone, and driving a car that needs little to no human input. The convenience and joy that technology has brought to the leisure and entertainment sectors of our lives has been exponential, and tech as a whole has become very much ingrained in our daily existence. In addition to this, tech has also become a large agent within the security business, particularly in the industry of Cybersecurity. But as with all good things, there is always another side to the metaphorical coin. In this case, I would like to narrow down the technological realm to the world of Biometrics. At first glance, this term may be unfamiliar to those that are not either already somewhat involved in the world of Cybersecurity already or even just the tech scene. However, this seemingly foreign concept has surely been interacted with by a majority of the current population, whether they have realized it or not. Biometrics is an umbrella term that refers to "a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition" (Department of Homeland Security). In short, Biometrics is a term that describes using physical features as a form of identification, often for security purposes. Some common examples of Biometrics are fingerprints, iris scanning, and facial recognition. These forms of biometrics are often used in higher-level forms of security, such as with the Department of Homeland Security and the within the Healthcare Industry, but even the Face ID that is used by virtually all people that own an iPhone would very much be considered a form of Biometrics. On the surface, Biometrics appears to be a wonderful advancement in security technology, as the convenience is unmatched and the idea of using features such as iris scanning, and facial recognition seems to be the works of a science fiction movie. But this is no feature film and there are very real issues with the usage of Biometrics on multiple levels. Biometrics as a concept begins to blur the lines between what is ethical and what is not when it comes to methods of security. The major issues that make Biometrics something that you may want to avoid are lack of user consent, critical concerns regarding privacy, and the overall dangers due to the sensitive nature of biological data.

In order to fully understand the issues that are apparent with Biometrics, it is imperative that an individual has at least a baseline understanding of its history and conception. Though on the surface it seems to be a relatively recent invention/concept, Biometrics have actually been around for multiple centuries. At the earliest, ancient civilizations had scriptures and writings that featured the usage of features such as fingerprints and handprints as a sort of signage, which means that these would be the first sightings of what could be considered Biometrics by definition. In the late 19th century, the development of Biometrics took the next step with the implementation of the practice as a proper instrument for the purpose of identifying people and a security method due to the labors of Alphonse Bertillon. Moving much farther into the future, the first forms of fingerprinting systems were made and distributed into the world around the early 1900s. This indicates the development of security-based systems that were centered around the usage of physical traits in order to grant authorized access. The more modern and sophisticated forms that are commonly used today such as iris and facial recognition came into existence around the late 90s. Since then, these systems have become used world-wide and are present in various industries including border control and law enforcement. In addition to the current forms that are in existence, the most recent updates to Biometrics have seen things such as artificial intelligence and complex algorithms contribute to the growing practice. Now that we have covered a brief history of the concept, the next step is to address the problems with it and why I am a detractor of Biometrics.

For the stark opponents of Biometrics, privacy has become one of the biggest points of contention. Privacy in the digital world in general has always been a bit of a murky subject. To start things off, there is currently no dedicated legislation towards protecting privacy within the United States on the federal level, unlike the UK or other countries. This goes to show how much of a still-contested issue privacy is, as a superpower such as the United States lacking in this category is not a good sign. This alone opens the door for a lot of misinformation regarding how Biometrics can be used and the rights of the people who are having their biological data recorded in the United States. In particular, there have been concerns regarding the collection of biological information without properly stating the purpose. This sensation is known as "function creep" and can lead to the mishandling of biological data without the individual's being informed about what their data is being used for. These hidden secondary purposes pose a major ethical issue with the collection of data, and therefore contributes to the larger issue of privacy with Biometrics as this can be considered a major betrayal of client trust and an overall invasion of privacy. Another major point of contention with Biometrics is the issue of consent when it comes to the covert means of collection biometrical information. For the more commercial means of collection, there is a clear and often concrete form of user consent given to whatever company is providing Biometrics as a form of security or authentication. An example of this would be Apple users agreeing to the terms of service that come with using face ID to unlock their iPhone. Once the agreement has been checked off, the user then additionally consents to having their facial features scanned and stored onto their phone's database and the apple database on a larger scale. However, there are more covert and undercover means of data collection that happen without the meaningful consent of the users involved. Because of the nature of this collection, it is often impossible for the users to agree to this, and therefore this would be considered an unethical practice, despite the fact that it is often done with security and safety being the main priority. The third and arguably most alarming problem with Biometrics stems from the fact that biological information in itself is an extremely sensitive form of data and collecting it for any means may not be safe for any client. Imagine the scenario where a malicious hacker is able to gain unauthorized access to one of your accounts due to them being able to locate and harvest your password through some sort of cyber-attack. The damage may have been done in terms of your account being temporarily compromised and some data being downloaded, but at least you can simply go the route of changing said password and hopefully strengthening it in order to prevent this sort of incident from happening in the future. There are also tons of guidelines and tips on how to have a good password with the necessary components to avoid detection. Also, passwords can be optionally updated whenever the user chooses which most Cybersecurity specialist would tend to recommend people to do so, even in the absence of an attack. Now imagine this same scenario, but with the password being switched out for biometric data, such as a facial scan. This situation would prove to be much more damning, as your actual facial data is now in the hands of ill-meaning criminals and cannot simply be changed. Once the hackers have this type of data, you are now in danger of falling victim to things such as impersonation and identity theft and may not be able to recover fully. So, to avoid such a dire situation, it may be in the best interest of everyone to completely avoid having your Biometric data collected by any means, even if this means sacrificing some of the benefits that Biometrics can provide. In the end, the risk involved with Biometrics are not worth it in the long run and there are other forms of security authentication that do not infringe on personal privacy and ethics in the same manner.

In order to truly perform an in-depth analysis into the topic of Biometrics and its ethicality, I would be remiss to not acknowledge the potential counterarguments that could be made in favor of it. There are positives that have been brought about by the emergence of Biometrics and multiple reasons as to why it has become such as commonly used concept. This includes things such as unmatched convenience and relative reliability. When it comes to convenience, there is currently nothing that even comes close to what things like facial recognition and fingerprint reading can offer. Instead of being forced into formulating a multi-faceted passcode or a complex pattern that you have to remember in order access your bank account, you can simply present your eye to a scanner or camera and immediately be granted access. But as I had alluded to in the previous paragraph, this convenience comes at a very large cost, as the type of recovery plan that can be enacted in the case of lost biological data pales in comparison to what can be done to salvage a stolen password. In this instance, the sacrifice being made for some extra ease of use is simply not worth the potential consequences. Next, there is the counter argument that Biometric methods have proven and high rates of reliability. But the issue with this so-called reliability lies in the fact that there has been extensive incidents of what are called "false positives", which counteract the seemingly fool-proof method of authentication boasted by Biometrics. A "false positive" is simply any type of error made by the system regarding an input not matching the set template, but access being granted anyway. On the other side of this, there are also instances of false negatives, which is when the system is not able to find a match between the matching template and the input. These errors greatly compromise the overall integrity of Biometrics and put the notion that it is a completely reliable and "fool-proof" form of security authentication, neatly and promptly to bed.

In conclusion, is important that a widespread discussion of Biometrics be had by the world, as this is without a doubt a global issue that will continue to grow due to the current rapid trajectory of technology advancement. Due to how much Biometrics has expanded in world reach and overall usage to the present, its problems affect and pertain to major companies, all the way down to your average Joe. While doing my research, I was able to find a reasonable number of sources with accounts sharing the same level of concern regarding Biometrics as my own. However, the majority of the world still seems to either be oblivious to the dangers presented by this method or otherwise completely indifferent to the issue. In my opinion, Biometrics are dangerous and should be widely avoided by all that can help it. Issues with Biometrics include but are not limited to privacy concerns, limited opportunities for clear user consent, and ethicality concerns regarding the sensitivity of biological information. When it comes to privacy, Biometrics often fail to protect the rights of their users, as there are many instances of data collection resulting in misuse of said data or even the revealing of information that was not originally intended. For consent, there is a distinct lack thereof, as many forms of covert data collection for Biometric means are not able to provide ample opportunities for consent to the individuals at stake. And to top it all off, the very nature of any type of biological data means that it is dangerous for it to be collected, even if seemingly for protection and security.

Annotated Bibliography

Woodward, J. D., Webb, K. W., Newton, E. M., Bradley, M., Rubenson, D., Larson, K., Lilly, J., Smythe, K., Houghton, B., Pincus, H. A., Schachter, J. M., & Steinberg, P. (2001). WHAT CONCERNS DO BIOMETRICS RAISE AND HOW DO THEY DIFFER FROM CONCERNS ABOUT OTHER IDENTIFICATION METHODS? In *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns* (1st ed., pp. 21–32). RAND Corporation. http://www.jstor.org/stable/10.7249/mr1237a.11

This source is taken directly from a textbook chapter that covers Biometrics and its distinctive features particularly from a military perspective and is written by an array of authors: Woodward, Webb, Newton, Bradley, Rubenson, Larson, Smythe, Houghton, Pincus, Schachter, and Steinburg. From what I could find, the author credentials appear to be that they are a mix of cybersecurity professionals, IT professionals, and college professors. From reading this source, I learned about the concerns that even the military had regarding the ethicality of Biometrics, which is significant because their operations are more prone to willingly compromising these ethics. In addition to this, specific issues regarding sociocultural concerns were talked about, which greatly contributed to helping decide which three issues I wanted to focus on in my paper.

Grimes, R. (2022, November 8). *The problem with biometrics*. LinkedIn. https://www.linkedin.com/pulse/problem-biometrics-roger-grimes

This source is an article written by Grimes, who is a current Cybersecurity Professional working for the company KnowBe4. In the article, Grimes gives a brief description regarding what Biometrics are and then proceeds to delve into the different challenges surrounding the controversial topic. This includes accuracy, hacking potential, dangers of stolen biometric data, and privacy issues. The perspective given by this article was valuable, as it provided a contrast to the militaristic view that was presented by my first source and was more geared towards a general audience. One of the key takeaways from this article was the focus on privacy as an issue, as this contributed to it being one of the major issues I had for my paper.

Boone, G., Huang, J., de Spiegeleire, S., & Sweijs, T. (2009). *FUTUTRE ISSUE BIOMETRICS: The Uncertainty of Identification & Authentication: 2010–2020*. Hague Centre for Strategic Studies. http://www.jstor.org/stable/resrep23999

This source is a research report that covers the issue of Biometrics and how they project into the future. The authors for this report are Boone, Huang, de Speigeleire, and Sweijs. From what I could find regarding author credentials, de Speigeleire is an author and scientist, Huang is a researcher in the field of cybersecurity-related issues, Sweijs is the Director of Research at the Hague Centre, and I was not able to find specific information regarding George Boone, but he appears to also be an author and researcher as well. All of these authors collaborated in conjunction under the Hague Centre for Strategic Studies to produce this research report. This source proved to also be quite valuable, as it provided research-based foresights into Biometrics, which allowed me to further build upon the foundation by which I was taking the anti-Biometrics side and it also addressed the privacy and security issues as well, though on a smaller scale compared to the other sources.

Thales Group. (2023, March 1). *The history of biometric authentication*. Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-biometric-authentication

This source was a webpage derived from the website of a French IT company specializing in electrical systems and technological equipment for a variety of industries. The webpage had no directly credited author, so the credit would fall to the company itself by default, and the company's credentials are that it is a multi-billion-dollar IT company that can be expected to have expertise in the field. The webpage provided an extremely detailed insight into the origins of Biometrics, as well as how it has grown and developed over the years. This helped for the purpose of contributing context and history of Biometrics, as required in the research paper. Additionally, the source provided the perspective of a French company, which was nice considering I was trying to emphasize Biometrics being a global issue throughout the paper.

LANGENDERFER, J., & LINNHOFF, S. (2005). The Emergence of Biometrics and Its Effect on Consumers. *The Journal of Consumer Affairs*, *39*(2), 314–338. http://www.jstor.org/stable/23860610

This source is a journal article derived from "The Journal of Consumer Affairs", written by the authors Langenderfer and Linnhoff. Langenderfer is a professor of Marketing and Law at Meredith College School of Business and Linnhoff is an associate professor of marketing at Murray State University to sum up their credentials. This source was valuable because it provided insight on Biometrics with emphasis on how it effects consumers. It discussed its advantages for business and consumers alike, which contributed to my paragraph about the counterarguments for the positives of Biometrics. The source then discussed the potential negative consequences and how dangerous they could be, which contributed to my overall stance on the topic.

Office of the Victorian Information Commissioner. (n.d.-a). *Home*. Office of the Victorian Information Commissioner. https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/

This source was a webpage derived from a website run by the Office of Victorian Information Commissioner, which appears to be related to the Australian government. This source had no named author for the webpage, so I would assume that the author was an employee for the organization. The source itself covered Biometrics and the problems and issues that it has with preserving privacy of those that are involved. Additionally, the source gave insight regarding how the authentication system works, and the different uses for it. The section focusing on privacy greatly contributed to my research paper, as I had privacy as of the main points of contention regarding why I think Biometrics are dangerous and should be avoided.