CYSE 425W Policy Analysis: Societal Issues over Privacy with Biometric Technology

Alysia Beckles

Old Dominion University

CYSE 425W Policy Analysis: Societal Issues over Privacy with Biometric Technology

**Introduction**

Over the past decades, the way that society functions have considerably changed. As technology advances, its impacts on society have become more prevalent, whether it relates to communicating with others, executing tasks, collecting information, and other capabilities, it is part of their daily lives. Implementing technology is meant to improve society. Technology could provide something as mundane as making a cup of coffee to something as complex as managing the operations of a facility remotely. Biometric technology's purpose was to aid in verifying users who are trying to gain access to a system or building in an efficient manner. There are various techniques to capture biometric data, such as fingerprint, iris, and voice. Biometric technology is gradually being adopted all over the world since it is convenient for society to use since all people have to scan their physical attributes, and not time-consuming. Although biometric technology was created as an alternative to the traditional method of verifying and authenticating people, there have been some tradeoffs with biometric technology regarding privacy and security.

**Biometric Technology Privacy vs Security**

There have always been issues surrounding security and privacy since maintaining security seems to be at the forefront. Although the terms used interchangeably, privacy applies to people's ability to manage their personally identifiable information, while security applies to protecting that type of information from anything that is a threat (Brad,2022). Proponents of biometric technology argue that it will give society more protection since it will thwart potential threats from obtaining unauthorized access to their personally identifiable information. Biometric technology offers advanced levels of security meant to assure users. In order to secure their information, people who utilize their biometric data to gain entry to a system or building will not need to memorize a complex password that may need to change routinely. Its authentication process creates an obstacle for potential threats since usually only actual authorized people can circumnavigate. When utilizing a traditional method for authentication, potential threats can gain access by guessing a random combination of numbers or knowing their significant other's name. With biometric technology, potential threats will need people's fingerprints instantaneously, and they will have to utilize specialized techniques to obtain that data. Although biometric technology's purpose is to dissuade potential threats from accessing personally identifiable information effortlessly, this technological advancement has caused issues regarding privacy.

Biometric technology will infringe upon their privacy since it facilitates the surveillance of society Maintaining information privacy is crucial. Informational privacy is when people have the right to restrict the accessibility to personally identifiable information that could expose their identity (North‑Samardzic, 2019, p.439). There is a constant struggle between security and privacy in society. The balance between privacy and security regularly shifts in reaction to anticipated threats (Goel, 2015, p.26). However, biometric technology is against society because privacy concerns arise when companies store biometric data that unauthorized third parties can use.

**How Biometric Technology Impacted Society regarding Privacy**

Biometric technology will violate people's privacy since there is a possibility that once they use their fingerprints in the system, a forensic database could utilize that type of data for a variety of unwarranted reasons. A possibility could that their personally identifiable information will be used against them by companies or other entities. Biometric technology is not infallible, and an important vulnerability distinctive to biometrics technology is the acquisition of stored biometric data by those who plan to misuse it. Once a company or any other entity capture that data, people cannot use a new set of fingerprints or irises since that type of information is a unique identifier. Although the purpose of biometric technology is to provide a higher layer of security, compared to traditional methods of authentication, biometric data cannot get canceled since it is permanent (Abdallah et al.,2015, p.65). Once that type of information is taken unauthorized individuals will gain access to sensitive information that calls for biometric authentication. Biometric data will disclose personally identifiable information such as health condition, age, ethnicity, name, and gender.

There have been instances when law enforcement uses biometric databases to prosecute people. Currently, there are companies that collect their consumer’s biometric data to help them discover their ancestry. Then, they will store it in a database. Once biometric data is exposed to a third party for reasons other than the services mentioned, privacy concerns arise. There have been some examples of companies providing ancestry services giving biometric data to law enforcement. This is an issue since people who use their services do not give the company permission to share personally identifiable information. Law enforcement will have access to anybody’s biometric data and utilize it for investigative purposes. Law enforcement will upload biometric data from a crime scene to a database and try to find the exact match. If the people that law enforcement is searching for do not utilize the database, oftentimes, the closest match will come up, displaying relatives (Ness, 2020). Then subsequently, the biometric data will get traced to the suspect. Law enforcement can take this action since it is not seen as an infringement on people’s right to privacy. Legally, there are no laws preventing law enforcement from doing so. Compared to how law enforcement traditionally gets evidence on people, they can discreetly obtain biometric data without a warrant. (Ness, 2020). When people sign up for these services, they expect that people working in the company will only be privy to their biometric data and will only use that information for the services specified.

**Conclusion**

The arguments stated in this essay demonstrate that, although biometric technology provides an extra layer of security, it has developed flaws by neglecting privacy. Regardless of authorization from people, law enforcement can ask for any database and have access to anybody’s biometric information. People who are not consumers of ancestry services will still have issues with privacy since it only takes one person that they are related to identifying who law enforcement is looking for. Privacy is a prevalent issue since the biometric data stored in a database is stored, and people do not know if using it will be used against them for criminalization.

**References**

Barros Barbosa, I., Theoharis, T., & Abdallah, A. E. (2015). On the use of fingernail images as transient biometric identifiers. *Machine Vision and Applications*, *27*(1), 65–76. https://doi.org/10.1007/s00138-015-0721-y

Brad. (2022, November 19). *Why is data privacy important?: Expressvpn blog*. Home of internet privacy. Retrieved December 3, 2022, from https://www.expressvpn.com/blog/why-you-should-care-about-privacy/

Goel, S. (2015). Anonymity vs. Security: The Right Balance for the Smart Grid.*Communications of the Association for Information Systems, 36* (2), 23-32.https://doi.org/10.17705/1CAIS.03602

Ness, L. V. (2020, February 20). *DNA databases are boon to police but menace to privacy, critics say*. The Pew Charitable Trusts. Retrieved December 3, 2022, from https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/02/20/dna-databases-are-boon-to-police-but-menace-to-privacy-critics-say

North-Samardzic, A. (2019). Biometric technology and ethics: Beyond security applications. *Journal of Business Ethics*, *167*(3), 433–450. https://doi.org/10.1007/s10551-019-04143-6