Essay 4 - Identification and Biometrics

During the last two decades, technology has evolved passed many people's expectations. There are self-driving cars, wearable technology, chip technology, new security identification and biometrics system, better hospital machines, electronic money, virtual reality and so much more. When it comes to identification in terms of Information Technology, it means the way in which or method used to recognize and individual or object. Identification checks can take place or can occur when devices and/or programs are used to read and recognize the individual or object. To identify an object a program is used to for example filter through an array of numbers to identify or recognize people's ID numbers. However, with biometrics, this refers to the, "physical or behavioral human characteristics to that can be used to digitally identify a person to grant access to systems, devices or data." (Korolov, 2019) For example, doing an eye retina scan to allow only authorized persons into a specially marked area in a business. Another example can be a fingerprint scanner where an individual scan their fingers in the immigration part of the airport for identification.

There are many benefits to using biometrics for identification purposes in this new technology era. It helps to amplify security in businesses and devices so there would not be any unauthorized attackers. However, when it comes to different types of biometrics and their benefits, some systems have an advantage over others. Biometrics has two categories; physical biometrics includes any physical characteristics of an individual such as face, fingerprint, hand, iris and DNA while behavioral biometrics has characteristics such as voice, keystroke,

signature and even an individual's gait. One benefit with using the physical biometrics of DNA is that its very hard to get a person's DNA from them to access unauthorized things whereas anyone can obtain a fingerprint pattern using special tricks and tools to make a copy print.

However, some biometrics systems are not as reliable as other identification methods. Sometimes the technology can glitch or lag. For example, sometimes the face recognition on a simple smart phone lock screen may not recognize the owner of the phone if the person had a need hair cut or change in makeup or it can simply be that the camera was not focused enough to scan the person's face. Sometimes sweaty fingers and palms can cause the fingerprint scanner or the hand scanner to not recognize the authorized people.

Another fault with biometrics systems are the privacy issues. Some people may get chip technology implanted in them containing information about there selves or other things. This technology chip be dangerous to a person's health. It can cause radiation or discomfort. It can also have the benefit of sending signals to identify who the person is. However, it can be a breach of privacy if the chip has been implanted illegally or if others monitor those who have the chips for other reasons while identification.

Hence, some users of biometric systems be unethical and breach of privacy of individuals. However, biometrics systems have both benefits and weaknesses but since technology has not developed well even, the weaknesses or faults of biometrics can be heavily noticed.

References

Korolov, Maria. 2019. *What is biometrics? 10 physical and behavioral identifiers that can be*

    used for authentication. February 12. Accessed November 17, 2020.

    https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-

    biometric-data-is-risky.html.