Surveillance State

Student Name

University Affiliation

Date of Submission

Introduction

Surveillance is regarded as an approach that is used to monitor the different behaviors, activities, and information to gather information, manage, influence, and direct. It takes different forms and can even include observation from afar through electronic equipment such as using closed-circuit television (CCTV). Surveillance is used by the state for intelligence gathering of information, preventing crime, protecting different processes, and investigating crime in different ways (Marciano, 2019). On the other hand, there are different ways that the state used to carry out surveillance. Some of these approaches include computers, telephones, cameras, social network analysis, biometric, corporate, wireless tracking, and the internet of things. The research focuses on understanding the use of biometrics in a surveillance state and their impact on human privacy.

Biometrics

Biometric surveillance is featured as a form of technology known for measuring and analyzing human behavioral and physical characteristics to identify, authentic, and screening. Some of the physical features captured in Biometric surveillance include DNA, fingerprints of a person, and facial patterns. On the other hand, the expected behaviour traits included in this process include the walling style of an individual (gait) and the voice of a person (Toor, Wechsler & Nappi, 2019). Facial recognition is regarded as a way used for the configuration of a person's facial features so that they can be accurately identified.

Why the use of biometric surveillance?

There are different reasons why the state is known for using biometric surveillance in the different approaches. Firstly, biometric recognition is significant for creating the required links between an individual and the different data records. Behavioral and physical characteristics are featured to b unique for every person. Therefore, they cannot be recreated or deciphered through hacking software (Willoughby, 2017). Secondly, biometric authentication is known to thwart the different efforts of fraudsters in the creation of multiple fake identities. Hence, biometric is featured to be very hard for the creation of other identities that can be used.

Thirdly, biometric surveillance is used as a result of biometrics not being able to be exchanged. Notably, fingerprints cannot be transferred. Biometric is a feature to be effective in protecting sensitive information such as healthcare records of individuals (Willoughby, 2017). Fourthly, biometrics is essential for being used in open banking as they require reliable digital identity protection for maintaining the different customers' information (Marciano, 2019). Banks have focused on using biometrics to increase their different online products. Therefore, biometric surveillance cannot be replicated.

Fifthly, biometric is known to have the ability to balance convenience, user experience and security. There are no other ways that these can be achieved using the other forms of security. In most cases, there are higher chances that the user can forget passwords and pins, but facial recognition will always be available. Biometrics is essential for providing exactly what the consumers want (Toor, Wechsler & Nappi, 2019). Sixthly, inborn biometrics are regarded to be significant and cannot change. The state is essential for ensuring that the different inherent biological changes cannot be changed. Lastly, it is essential to note that the surveillance state uses biometrics due to challenges if one uses the stolen biometric data. Biometrics are sophisticated and cannot allow one to sue stolen biometrics more effectively than typical biometrics.

Negative effects of Biometric Surveillance

Different disadvantages are linked to the use of biometric surveillance. The first disadvantage regards to privacy of an individual. It is noticeable that biometrics often pose the most considerable risk to privacy due to the government using it in the process of carrying out surveillance (Toor, Wechsler & Nappi, 2019). As a result of using face recognition technologies and becoming more effective through the use of cameras that can record more significant information, identification and tracking could become the norm in various settings. Secondly, the extensive collection of different biometric collections quickly increases the risk of compromised data that can be very hard to recover. Biometrics is likely to be used in various social security numbers (Willoughby, 2017). When such information is compromised, it is tough for that information to be recovered. Lastly, biometric faces challenge associated with a physical disability. Some of the individuals tend to be not fortunate enough to be enrolled in the process. This is as a result of losing or have damaged body parts. Therefore, these kinds of people are likely to find it hard to cope with this surveillance process. Hence, it is essential to ensure that the system is used most appropriately. Biometric surveillance is known for being viewed as the biggest threat to human privacy.

References

Marciano, A. (2019). Reframing biometric surveillance: from a means of inspection to a form of control. *Ethics and Information Technology*, *21*(2), 127-136.

Toor, A. S., Wechsler, H., & Nappi, M. (2019). Biometric surveillance using visual question answering. *Pattern Recognition Letters*, *126*, 111-118.

Willoughby, A. (2017). Biometric surveillance and the right to privacy [commentary]. *IEEE Technology and Society Magazine*, *36*(3), 41-45.