Ethics Of Security And Surveillance Technologies

With the innovative ways of technology, the dynamics of the current environment, the need to fight terrorism, national security, and privacy concerns in respect to rights and justification, the gravity and nature of electronic and Internet surveillance have increased in recent times, which has sparked debates on ethics and surveillance. This issue has been at the forefront due to the vigorous use of modern technology in surveillance and the complexity that surrounds it. As we accept how technology has and continues to transform and revolutionize the way we live, it also presents substantial challenges in our operations especially security and our privacy. These have been issues that need to be discussed and addressed in policy and decision-making as well as laws and policies.

With the innovation of technology and the wider use of the internet to include social media platforms, electronic surveillance has been on the increase due to the significant number of information collected. Over the past 15 to 20 years, state governments have been using various means and platforms to surveil and monitor their citizens using complex surveillance tools. Technologies such as video and audio recordings, databases, social media platforms, and other technologies are invading the privacy of more people. As threats continue to increase and the nature of our environment changes due to proxy wars, and national security, the innovations of technologies have become more innovative and advanced.

As technology, continue to advance, the abilities of governments to monitor their citizens increase. This has raised and brought about ethical concerns in regards to surveillance and people's privacy. In terms of collection, technology has been extremely good in monitoring real-time events but the ethical issues recently must be addressed and weigh the outcome of surveillance and the need to protect people's privacy.

While technology is its advantages and disadvantages, technology has caused many ethical problems as a result of either negligence or the misuse of complex surveilling equipment. While the debate and argument continue to grow with no absolute conclusion and ethical issues continue to rise whiles government continues to strengthen its security, the need to balance ethics and surveillance must be addressed to bring stability. In this review of the literature, we will examine the ethics of government monitoring in regard to the privacy and national security.

The comprehensive increase in terrorist acts since the September 11, 2001 (9/11) attacks in the United States have surely helped focus on the need for surveillance equipment to protect people and their society. Over the past years and essentially from the 9/11 attacks, complex surveillance equipment has vividly increased across a wider spectrum of areas that directly or indirectly influence and likely affect people's daily operations. With the huge advancement of technology and the need to combat and prevent terror, organizations and government agencies have the ability to maintain a more comprehensive vision of people's actions using the internet and social media to track information, movement, etc. using surveillance to collect a huge amount of data. Within the data-profiling sector, it may be a surveillance mission due to developments and innovations in electronic surveillance that have contributed to massive growth in personal life, ethics, and the way data is collected. Supposedly, databases held by government organizations as well as business organizations might be connected to other user

systems, which may raise ethical concerns.

The ethical concerns surrounding electronic surveillance look likely to increase with the innovations and advances made with respect to technology. Within these issues, there probably needs to be a connection or relationship between practical and logical ethical standards. Therefore, governments and organizations ought to consider this when making decisions concerning electronic surveillance.

Data collection may be collected in numerous ways. Law can require it provided law enforcement agencies follow all protocols to get approval from the attorney general. The issue facing the collection process is to determine the ethical necessity of the information gathered and avoid any obstacles to human rights.

Privacy encompasses surveillance, collecting, and keeping the information in its anticipated range. When information is moved outside or further than its planned range unintentionally or viciously, privacy is breached and ethical concerns are raised. A breach of privacy may occur when information is shared with a party for whom it was not intended and may occur when information is abused for a different purpose other than what it was intended.

The conception of risk regarding information privacy has been suggested as a precursor of information privacy concerns (Dinev and Hart 2006) and is often defined as the degree to which an individual perceived potential for a loss associated with personal information (Featherman and Pavlou 2003). Smith et al. (1996) explain the extreme usage of personal information damages people’s privacy in some essential ways. The inappropriate use of personal information is due to a lack of proper privacy measures and controls. In addition, the unapproved use of personal information without the personal consent for the purposes external to the original purpose (Culnan 1993).

Currently, a major concern on privacy is how young adults or teenagers are freely giving out information through social media mostly without any privacy settings. Marwick, Murgia-Diaz, and Palfrey (2010) specify that young people are viewed as a generation that is depicted as being more comfortable with technology and hence different ideology compared to adults. A publication by Dratwa (2015) present different views and addresses the concerns of surveillance and security as well as privacy from an ethical view. Data continues to present the legal and authority from the European perspective on how technology has the potential to intrude on people’s privacy and why states or organizations require a case-by-case justification. In addition, Dratwa enforces why states must be accountable for their actions whiles measures are put in place to monitor compliances.

The Ethics of Surveillance (Macnish, 2017) portrays how sometimes surveillance may be good or bad depending on the situation. Macnish explains how different situations are used in surveillance that bring about some ethical issues in each instance. Macnish further explains the rationale behind surveillance used by organizations and the effects it brings.

The continuation of threat and the increase in adversary’s complexity has given rise to more surveillance on the Internet using much-sophisticated technology. Although authorizations are given to agencies to monitor and protect national security, much of the process is abused which hinders people's privacy as well as ethical issues. Bellaby (2012) provides a strategic framework of how intelligence monitoring adopts to the changing environment and new

emerging threats on the current environment. Bellaby further explains how abuses of some detention facilities such as Guantanamo Bay have increased the use of technological surveillance and using torture as a means to gather intelligence and thus the need to make a clear policy on intelligence practices to mitigate ethical issues. Ashcroft (2007) provides insight, analysis, and authorized the Federal Bureau of Investigations to conduct investigations based on threats to national security by collecting foreign and domestic intelligence using all abilities and techniques to protect the United States from threats.

The standards of reasonable practices are outdated and require the need to be expanded to accommodate new innovations to include surveillances (Marx, 2006). Marx discusses that; the use of surveillance to monitor people should be based on the means. In addition, Marx outlines some conditions such as not seeking the right approval may be considered a breach of an individual's privacy.

Years after the 11 September 2011 terrorist attack on the United States, issues of information surveillance and collection between the intelligence communities were raised due to ethical issues. After the outcome, policies and laws were passed to increase surveillance and collection methods. In addition to this, there have been amendments to the Foreign Intelligence Surveillance Act as well as the Patriot Act. The Foreign Intelligence Surveillance Act (FISA) establishes procedures and authorizes the use of electronic collection methods of foreign intelligence (Meason, 1990). Also, the FISA Court was established to approve the use of electronic surveillance for foreign intelligence purposes (Meason, 1990).

In the past few years, due to leaks and domestic issues relating to terrorism and espionage, the Attorney General issued guidelines, which gave liberty to the FBI to use technical methods in intelligence collection. As such, data and information may be obtained without the approval of authority if a situation is imminent. Under the guidelines of the Attorney General, the FBI may have overreached stepped their boundaries in collecting data.

In an October 2018 ruling unsealed and posted on October 8, 2019, by the Office of the Director of Intelligence, the United States Foreign Intelligence Surveillance Court (FISC) found that the employees of the Federal Bureau of Investigation had inappropriately used data collected under Section 702 of the Foreign Intelligence Surveillance Act (FISA). The FBI was found to have misused surveillance data to look into American residents, including other FBI employees and their family members, making large-scale queries that did not distinguish between US persons and foreign intelligence targets" (Gallagher, 2019).

Finding the balance between security and privacy is hectic for the government due to national security issues. As long as collected data does not become the norm of the day, it may be okay for citizens to feel safe if personal information is not used against them and instead used in crimes and fighting terror. This will bring about trust between the people and the government. According to Pulver and Medina, "it is important to evaluate the people's trust in the government, as mistrust can lead to national security issues. The public has been informed through media, to some degree, of these alleged intelligence collection programs and they are concerned with governmental surveillance".

History predicts that after an attack on the homeland, laws, and policies are passed and tightened to prevent another attack. In this review, after the September attack, the authority was given to law enforcement agencies and organizations to use electronic surveillance to collect

technical communication and analyze intelligence, both domestic and foreign in order to combat terror. With the advance in technology, more capabilities are developed and surveillance and collection processes have infringed on individuals' privacy in recent years. The use of social media platforms has also made it easy to gather information. Although those data are private and not ‘releasable’ to the intelligence community for intelligence purposes, that information is stored and used to provide security measures. In addition, the Snowden leaks increased awareness on privacy issues as well as more security measures in place to prevent further and more leaks.

Intelligent agencies and the Attorney General must take practical and realistic percussions to protect personal information derived from the Internet especially United States persons. When personal data must be used, it must be relevant for the purpose, such as crime and terror activities. In order for all the security policies to be enforced, there must be compliances across all the agencies and intelligence communities and enough policies to protect citizens' privacy and rights whiles protecting national security. Finding the balance between ethics, surveillance, and collecting information continue to be hectic but there needs to be a system of oversight and vivid policies that must be based on how technology advances and the current environment.