The ethicality of the role engineers play in enforcing national security

Vidhur Potluri
UIN: 626007235
ENGR 482 Section 923

Introduction

National security is the mechanism put in place by a nation state to protect its economy, its institutions and most importantly, its citizens. In the United States of America, agencies such as the Central Intelligence Agency (CIA), The Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) have been established to overlook the country's national security. These agencies indulge in activities of counterintelligence and espionage to ensure that national security is protected. According to the Cambridge dictionary, counterintelligence means a "secret action taken by a country to prevent another country from discovering its military, industrial, or political secrets."[1] It includes activities aimed at preventing acts of espionage, sabotage, assassinations, etc. The Cambridge dictionary defines espionage as "the discovering of secrets, especially political or military information of another country or the industrial information of a business."[2] The office of the director of national intelligence, while describing economic espionage aimed towards America, notes that now "adversaries use traditional intelligence tradecraft against vulnerable American companies, and they increasingly view the cyber environment—where nearly all important business and technology information now resides—as a fast, efficient, and safe way to penetrate the foundations of our economy."[3] Dealing with such acts requires technology of the highest standard.

The technology that goes into these activities of espionage and counterintelligence has developed simultaneously with the development of the field of engineering and modern technology. It is obvious that these agencies require the best equipment, systems and devices

[1] "Counterintelligence." COUNTERINTELLIGENCE | Definition in the Cambridge English Dictionary, dictionary.cambridge.org/us/dictionary/english/counterintelligence.
[2] "Espionage." ESPIONAGE | Definition in the Cambridge English Dictionary, dictionary.cambridge.org/us/dictionary/english/espionage.
[3] "ODNI Home." Home, www.dni.gov/index.php/ncsc-what-we-do/ncsc-threat-assessments-mission/ncsc-economic-espionage.

to monitor any threats and prevent disasters. Engineers have always been at the forefront of developing devices that facilitate both national espionage and its adversary, counterintelligence. From the development of facial recognition software to the deployment of military surveillance drones, engineers have been behind it all. While the need for programs promoting national security is not often questioned, the means by which these programs operate have been under major scrutiny during recent times. Much of the software and spy craft used have raise alarms in the media and have been protested by the public in America at a large scale. It has come to light that the NSA has indulged in activities widely recognized as unethical for an invasion of privacy. This paper intends to discuss the role engineers play in espionage and counterintelligence and considers the ethics of such participation and development of controversial technology, mainly in the United States of America. It discusses only matters of national security, and not the widespread corporate espionage taking over America. It also presents some examples of technologies developed by engineers and how they've impacted intelligence gathering services, including the infamous case of PRISM and former CIA computer scientist Edward Snowden. This paper theorizes that in order to protect certain rights of the public, engineers need to limit the functionality of spying tools that they develop and have a responsibility to reveal any truths that may impede people's liberties. It also theorizes that although preventive ethics may compel NSA, FBI, and CIA engineers to hide the truth behind the technology that goes into national security, since they hold a responsibility to millions, they should adhere to the doctrines of utilitarianism, and thereby make calculated predictions about the consequences of their technology and follow the rules set in place by the Government to ensure the safety of the public.

From the perspective of different ethical ideologies

Kantianism states that an individual's moral philosophy should be based off an a priori method, and not their empirical knowledge. The third formulation of Kant's categorical imperative emphasizes that another person must never be treated as a means. Since the way national security is implemented by these agencies is majorly based off of looking into people's communications internationally and their internet searches, we can see that Kantianism would condemn such actions and deem it unethical. Furthermore, it can be inferred from Kant's law of autonomy that privacy and autonomy is of utmost importance, and the development of

programs such as PRISM (discussed below) by the NSA engineers is highly unethical according to Kant's duty ethics. Although most of these programs are approved and finalized by officials in the NSA, it takes an engineer's mind to conceive of and implement such programs. Biometrics are discussed in depth in an article titled "Technology changing future espionage"[4] by an online news named 'SOFREP'. It states that "with the advent of biometric technology such as fingerprint scanners, widely used in airports and customs control points around the world, spies may need to adjust their tradecraft or develop entirely new techniques." The constant war between espionage and countermeasures to espionage, and the significance of the role technology plays in this war is well noted. Kantianism would disagree with any act of espionage or countersurveillance since it is highly likely that the act involves an invasion of privacy and a usage of citizens' information as a means to collecting information. Since experience is of utmost importance when it comes to judging whether the use of technology like biometrics is ethical or not, and the necessity of espionage and counterintelligence is unquestioned since the battle between the two had started ages ago, it is safe to disregard Kant's duty ethics to question the actions of engineers involved in national security.

J.J.C. Smart, in Oxford journals, defines utilitarianism as - "Utilitarianism is the doctrine that the rightness of actions is to be judged by their consequences."[5] This means that utilitarianism takes into account experience unlike Kantianism. The consequences of developing software used by intelligence agencies are multifold, but usually have either a positive or negative outcome and are not ambivalent. A lot of the intelligence gathering is based on chance. While sometimes, officials are looking for a specific piece of information or a threat (facial recognition), most of the time they're searching the internet and analyzing tons of data hoping to identify a threat or lead. NSA's PRISM software does exactly this. 'theverge.com' describes PRISM "as a tool used by the US National Security Agency (NSA) to collect private electronic data belonging to users of major internet services like Gmail, Facebook, Outlook, and others."[6] The program is used to search through American's emails, phone calls, and chats without a warrant. In addition to the obvious concern of an invasion of privacy, the PRISM program has caused discomfort to a majority of American citizens when the NSA participated in spreading

[4] "How Technology Is Changing the Future of Espionage." SOFREP, 7 May 2016, sofrep.com/news/technology-changing-future-espionage/.
[5] [5] J.J.C, Smart. "Extreme and Restricted Utilitarianism." *Oxford Journals*, Oxford University Press, 1956, p. 344.
[6] Sottek, T.C., and Janus Kopfstein. "Everything You Need to Know about PRISM." The Verge, 17 July 2013, www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

misinformation. They proclaimed that only international citizens were stripped of their right to privacy. However, it was revealed that PRISM was used by the NSA, CIA and FBI to read Americans' s communications which was an obvious violation of the Fourth Amendment. Edward Snowden, a CIA technical assistant and computer scientist working at the NSA, decided to leak some classified documents to the public and reveal top-level clearance information of the USA Government through an interview with the Guardian. In this interview, he said "My sole motive is to inform the public as to that which is done in their name and that which is done against them"[7] and claimed that he did nothing wrong.

Unlike Kantian followers, utilitarianists would believe only the outcome of such an invasion of privacy. If using PRISM allows the Government to pinpoint a threat, then the utilitarianists would judge the program ethical. They wouldn't consider the act of going through private data unethical unless it causes direct distress to a person. Furthermore, it is likely the two distinct groups of utilitarianists would perceive the program differently. Programs such as PRISM are generally protected by certain Government acts. Certain aspects of PRISM that are public knowledge and the secrecy with which the NSA and FBI act are protected by Section 702 of the Foreign Intelligence Surveillance Act. To rule utilitarianists, those that decide the morality of actions based on their adherence to rules, aspects of PRISM that comply with the law are morally acceptable. To act utilitarianists, however, PRISM is acceptable only if it is the best solution to hostile threats posed by adversaries of America. Edward Snowden believed that revealing confidential documents was the best course of action to bring about change in the way these agencies operate. Rule utilitarianists would condemn the actions of the intelligence agencies for non-conformity with the fourth amendment, as well as Edward Snowden for non-compliance with the regulations of the CIA and NSA. The case of Edward Snowden, who has since been in exile, underscores the importance of engineers' responsibility towards the public as well as the need for public support for engineers working in the Government.

[7] "Edward Snowden: the Whistleblower behind the NSA Surveillance Revelations." The Guardian, Guardian News and Media, 11 June 2013, www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Virtue ethics places an emphasis on an individual's character. The intent to commit acts of espionage is reprehensible according to virtue ethics since such acts would shape a person's character to be vengeful. In the article by SOFREP, the author describes the possibility of spies bioengineered in the womb to serve the purpose of espionage and counterintelligence. The article states that despite the possibility of such revolutionary technology coming into existence, it is quite difficult to grow human qualities in a lab. This is very relevant to virtue ethics since if DNA could be altered by engineers to create the ideal NSA or FBI agent with qualities of deception and anonymity, the effect of virtue ethics on such a person's thinking would be minimal. The interpretation of acts of espionage and acts of counterintelligence by virtue ethics is very different. While espionage involves deception indicative of a flawed character, counterintelligence involves responsibility towards national character indicative of a morally adept character. Since there is a lot of middle ground involved in virtue ethics' take on espionage and counterintelligence, a more apt doctrine of ethics in this case would be preventive ethics. Espionage intends to cause harm to public and disregards any guidelines set to prevent harm from occurring to public, regardless of the country. Preventive ethics places emphasis on preventing acts of espionage that cause harm to the public. However, the specific activities performed to carry out either espionage or counterintelligence (facial recognition, metadata, etc) and the amount of harm inflicted on the public by these activities is subject to discussion.

I consider myself a utilitarianist, bound to making decisions based off of their perceived consequences. I also tend to favor the more virtuous option when making impromptu decisions, not just in the field of engineering, but everyday life. This is why I've chosen to discuss in depth the merits and demerits of viewing the role of engineers in national security from the perspective of utilitarianists, and virtue ethics. While I am not an avid believer in Kant's duty ethics, I chose to discuss it because I've realized that its popularity is vast, even in the field of engineering. Preventive ethics' role in engineering can't be understated. The risk that engineers take increases as technology increases, and since I've understood its relevance, I deemed it necessary to discuss it.

Conclusion

Experience is crucial for engineers to work in creating technology used for counterintelligence

and espionage. They need to be aware of the consequences of developing products for agencies such as the NSA, FBI, or the CIA. When working with such agencies, engineers may not have access to crucial information because of the sensitive nature of the agencies' work or the lack of authority. Despite this lack of information, engineers need to operate with a sense of responsibility towards the public and understand the intentions behind the orders they receive to the best of their understanding. Engineers need to engage in risk engineering and evaluate all possible events that would have negative consequences because of the stakes involved. It would certainly help them mitigate the negative effects of their actions. Because of the nature of their work, engineers in the field of counterintelligence should adopt the precautionary principle that states "where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost effective measures to prevent environmental degradation." The costof failure is high in such an environment. An example of such a failure is noted in the SOFREP article where Hassan Mustafa Osama Nasr was kidnapped by the CIA from the streets of Milan under suspicion of recruiting Jihadist soldiers. The CIA operated under metadata obtained from Hassan's phone. However, it was later found that Hassan was innocent and the CIA officers were convicted by Italian courts.

With increasing rates of data tracking and cyber security, it is critical that engineers take important steps in regulating products created in the name of security. Drones, security cameras, and other espionage products used by governmental & privatized intelligence agencies are a serious threat. With so much of our user data already being tracked through our phones, one can only imagine what's possible with advanced face tracking in the future. It is important for engineers to find a perfect balance and consider the repercussions of every action they take.