The Ethics of Whistleblowing

Sudhan Chitgopkar

May 5, 2021

University of Georgia

sudhanchitgopkar@uga.edu

Contents

1 Intelligence as a Necessary Evil

Though intelligence organizations such as the CIA or NSA may seem as integral to the U.S. government as Congress or the Cabinet, it may be beneficial to consider the reason such intelligence organizations exist to begin with. As intelligence concerns itself primarily with the derivation of information for some consumer, intelligence and intelligence operations are neither inherently good nor inherently bad. They often exist as a means to the end of sound decision-making by some policy-maker, rather than an end in and of themselves. Some exceptions exist (i.e. covert action), though these too do not have inherent morality. On face, then, this topic seems relatively trivial. After all, how could it possibly be ethical for individuals to expose national secrets for an action that isn't expressly bad? Problematically, both the morality and ethics of certain intelligence operations are quickly muddied in practice as their theoretical moral neutrality dissipates. To better understand the ethics of whistleblowing, then, it is critical to understand why such aforementioned intelligence operations become ethically problematic.

In many ways, intelligence and intelligence organizations cast a beacon of light on the truth of realism in the world. As a result of the anarchic nature of international affairs, power-hungry states are often left to their own devices to ascertain power. In their pursuit of this power, each state is tasked with deciding whether or not they would like to conduct intelligence operations. This plays out as a prisoner's dilemma. While the best case scenario is a transparent world with minimal need for intelligence, each state's individual incentive to defect and carry out intelligence operations to gain an information advantage leads to widespread defection. In the status quo, this prisoner's dilemma defection is the norm. Unlike the traditional prisoner's dilemma wherein each prisoner is given a static choice, though, states today are able to determine how much time, money, and effort they want to invest in intelligence. This intelligence prisoner's dilemma, therefore, incentivizes states to dedicate more resources to intelligence than their competitors do. As a result, such intelligence

operations may become exponentially more extreme as states push towards the asymptote of intelligence effectiveness. It is here, on the sometimes morally and ethically ambiguous plane of intelligence operations, that the ethics of whistleblowing must be considered.

2 Contemporary Whistleblowing Legislation

As whistleblowing is an important means of reporting both fraud and wrongdoing, current legislation and precedents often encourage whistleblowing and protects whistleblowers from potential harm. Despite this, whistleblowing is a difficult and sometimes dangerous process, leaving whistleblowers that make even one wrong decision with little legal protection for their actions. Though the general definition of a whistleblower is understood as any individual that "reports waste, fraud, abuse, corruption, or dangers to public health and safety to someone who is in the position to rectify the wrongdoing, (National Whistleblower Center 2018)" there is no single legal definition for a whistleblower. The ethical standards for these whistleblowers are often defined by current legislation, though both a variety of precedents and norms also exist in this regard.

2.1 Evolution of Whistleblowing Legislation

Whistleblowing legislation in the United States can be traced back to the False Claims Act of 1863 (Pines et al 2015). This act, popularly known as the Lincoln Law, was a highly generalized piece of legislation that allowed whistleblowers to report false claims made by an organization for financial compensation and protection against being fired. Importantly, the act also held whistleblowers that made false claims liable for financial damages (Pines et al 2015).

The next significant piece of whistleblowing legislation was passed in 1978 as the Civil Service Reform Act (Berkebile 2018). Unlike the False Claims Act, this legislation only protected

federal workers and did not target whistleblowing specifically (Berkebile 2018). Rather, the Civil Service Reform Act sought to increase protections and benefits for federal workers as a whole, offering things like early retirement and codifying the prohibition of equal opportunity violations in the workplace. With respect to whistleblowing, the act was significant in its creation of the Merit Systems Protection Board (MSPB), which allowed federal whistleblowers to argue and potentially rectify any harm they suffered as a result of whistleblowing (National Whistleblower Protection Center 2021; U.S, Merit Systems Protection Board n.d).

The most significant piece of whistleblowing legislation was passed 11 years later as the Whistleblower Protection Act of 1989. This act extended whistleblower protections to private-sector individuals in addition to government workers and established much of the nuance that exists with current whistleblowing ethics (Whitaker 2007). Specifically, this act lays out important stipulations whistleblowers must meet in order to receive protection. Firstly, whistleblowers must be classified as "covered employees" (Whitaker 2007). While intuitively, this includes any current or past employees of an organization, the following groups are notably exempted from whistleblower status: employees of (1) the Postal Service, (2) Government Accountability Office, (3) FBI, (4) CIA, (5) NSA, and (6) any other "executive entity that the President determines primarily conducts foreign intelligence or counter-intelligence activities (Whistleblower Protection Act 1989)." Furthermore, only information that is not protected by law nor classified through an Executive Order may be released under the Whistleblower Protection Act (Whitaker 2007).

The Whistleblower Protection Enhancement Act of 2012 is the most recent bill pertaining directly to whistleblowers under the scope of this paper and seeks to modernize some aspects of the Whistleblower Protection Act of 1989. Most importantly, the 2012 enhancement now excludes the Office of the Director of National Intelligence (ODNI), and the National Reconnaissance Office from receiving whistleblower protections (U.S. Department of Justice 2019; Whistleblower Protection Enhancement Act 2012). Other notable changes include

giving whistleblower protection to employees of the Transportation Security Administration (TSA), and requiring a clause in non-disclosure agreements that informs the signer of their whistleblowing rights (Whistleblower Protection Enhancement Act 2012).

The most recent relevant legislation to this paper is the FISA Amendments Reauthorization Act of 2017. Like the Civil Service Reform Act, this act mentions whistleblowing somewhat transiently but is critical in that it allowed FBI employees to receive whistleblower protections, along with any "contractor employees" of the intelligence community (FISA Amendments Reauthorization Act 2017).

2.2 Legislation Analysis

By almost all measures of the law, whistleblowing seems to be an activity that is not only allowed but encouraged, as whistleblowers face little legal recourses and are often entitled to financial rewards for their actions. Few, if any, pieces of legislation exist expressly to denounce, harm, or otherwise criticize whistleblowers. Despite this, many whistleblowers in the intelligence field are labeled traitors (i.e Edward Snowden) and are excluded all protections for whistleblowing (Riechmann 2018). Here, the law seems to have a double standard. There are few situations where a whistleblower, even when making false claims, will face reprisal provided that he/she works in either the private sector or in a non-intelligence field. A member of the intelligence community, however, is not provided any protection (let alone reward) for alerting others of fraudulent, corrupt, or unethical action. On face, this legislation seems to dictate that whistleblowing is *always* ethical for employees of non-intelligence fields, so long as the information is not expressly secret. Antithetically, whistleblowing is *always* unethical for individuals that are a part of the ODNI, CIA, and NSA. Interestingly, though, contractors of any of the aforementioned organizations are provided whistleblower protections for the release of any non-secret information. *Why is this?*

The legislation and corresponding literature seems to indicate that secrecy takes priority to

oversight. If this is the case, though, what utility might there be in excluding intelligence agency employees from whistleblowing on any matter, secret or not? On a similar note, why are intelligence contractors (who may be privy to the same knowledge as intelligence employees) allowed to whistleblow on those same non-secret issues? These contradictions remain unaddressed by contemporary whistleblower legislation, creating a dangerous environment for would-be whistleblowers in the intelligence industry. Regardless of individual opinion, the vague intentions and seemingly contradictory nature of contemporary legislation provides little ethical guidance for potential whistleblowers. It is necessary, then, to look elsewhere to determine what such ethical principles might be.

3 Philosophy & Whistleblowing

As current legislation fails to dictate a framework by which to judge whether or not whistleblowing in a particular situation is ethical with respect to intelligence, such a framework must be sought out in philosophy.

3.1 Utilitarianism

From a philosophical standpoint, whistleblowing in the intelligence community is a nuanced topic. This is because intelligence work often seems incompatible with the pursuit of globally utilitarian principles. As mentioned in section (1), intelligence operations often represent an individual state's pursuit of information to get an upper hand. In that vein, intelligence is not conducted for the good of everyone, it is conducted for the good of one state and its citizens. In fact, intelligence can even be seen as zero-sum - when one state benefits from gaining information, it is only because another has lost the secrecy of that information. In this vein, it is not appropriate to consider the ethics of whistleblowing from a globally utilitarian perspective, as intelligence is often inherently not globally utilitarian. Specifically, it is unrealistic to argue that whistleblowing is ethical in any situation where an intelligence

operation is not globally utilitarian. That would expose state secrets at every turn of the road and likely lead to more harm than good - violating the very same utilitarian principle such an ethical perspective seeks to maintain.

3.2 Mills' Harm Principle

For this same reason, it is difficult to apply Mills' Harm Principle to intelligence. Simply put, Mills argues that an individual or organization is free to engage in any action they choose, so long as it does not harm others (Turner 2014). Using this principle as a guideline for the ethics of whistleblowing would mean that whistleblowing is ethical whenever an intelligence operation results in harm. As aforementioned, intelligence work is neither inherently good nor inherently bad. The prisoner's dilemma situation of intelligence today, though, incentivizes intelligence operations to be intrusive as a means of getting a strategic upper-hand. This often leads to at least one party being harmed in most intelligence operations. If whistleblowing was ethical when an intelligence operation caused any amount of harm, it would be ethical to blow the whistle on almost every intelligence operation conducted. Obviously, Mills' Harm Principle, in its most literal form, should not dictate the ethics of whistleblowing.

3.3 De George's Criteria

Recognizing the nuance of whistleblowing ethics and the inapplicability of just one moral principle to dictate these ethics, De George proposes five (5) specific criteria to determine whether a specific instance of whistleblowing is ethical (Hoffman and Schwartz 2015). The five (5) criteria are as follows: (1) the firm's actions will do serious and considerable harm to others; (2) the whistleblowing act is justifiable once the employee reports it to her immediate supervisor and makes her moral concerns known; (3) absent any action by the supervisor, the employee should take the matter all the way up to the board, if necessary; (4) documented evidence must exist that would convince a reasonable and impartial observer that one's

views of the situation is correct and that serious harm may occur; and (5) the employee must reasonably believe that going public will create the necessary change to protect the public and is worth the risk to oneself (Hoffman and Schwartz 2015).

Importantly, De George's criteria were not created specifically with intelligence in mind. Rather, they are meant to be a general set of guidelines for whistleblowers as a whole. As such, some criteria are ill-suited to intelligence as De George never considers the potential implications of whistleblowing on the release of national security information. Specifically, De George's fifth (5) criteria considers only risk to oneself, whereas whistleblowing on an intelligence issue may create a risk for an entire nation. As a whole, De George builds a strong foundations to determine if whistleblowing is ethical in general, but because this foundation does not consider the unique nature of whistleblowing in intelligence, it is not sound in intelligence applications.

3.4 Developing a New Framework

Though the aforementioned ethical frameworks by themselves are unable to determine whether or not whistleblowing is ethical in intelligence scenarios, each considers a unique aspect of this problem. Using all of them, such a framework may be created.

Utilitarianism dictates that actions are just if they result in the most amount of good for greatest number of people. In effect, this can be understood as maximizing benefits while minimizing harms. The reason utilitarianism, taken on its own, was ineffective as an ethical framework for intelligence whistleblowing is that intelligence inherently seeks to better only one group at the expense of others. Here, the scope is global as the effects of an intelligence operation are considered not only on the state conducting the intelligence action but also upon everyone else in the world. As established in section (1), though, intelligence is self-serving. For this reason, it would be more apt to consider whether or not an intelligence operation is utilitarian relative to its state. If the benefits of an intelligence operation

outweigh its harms for the citizens of the state conducting the intelligence operation, it is just. This is a significantly better framework by which to determine the ethics of whistleblowing in intelligence scenarios. Because a state is obligated to serve its citizens first and foremost, actions that harm citizens more than benefiting them can be seen as unethical. For this reason, it can be established that whistleblowing is ethical in cases where significantly more harm is done to a state's populace than benefits derived.

By itself, this utilitarian framework relative to the state is incomplete, though. Because this framework only considers actions within the scope of one state's population, intelligence operations which cause significant harm to others outside of the state could still be viewed as ethical. Mills' Harm Principle is therefore applicable here. While Mills argues that any action that harms others is unjust, adhering to such a strict standard is unrealistic for intelligence operations. Rather, a looser, more vague standard may be more applicable. Specifically, any potential harm to others should be minimized and within reason, with a specific focus placed on minimizing harm to any non-government agents. While enumerating exactly which harms are unreasonable and ethical grounds for whistleblowing is not feasible, literature on this topic is immense. Dictating these harms here would be tangential to this paper's purpose, but the author proposes that Article 8 of the Rome Statute in the Geneva Convention provides strong, well-defined guidelines of unjust harms.

Though a combination of both utilitarianism and Mills' Harm Principle provide a solid ethical framework for intelligence whistleblowing, neither utilitarianism nor Mills' Harm Principle take into consideration the uniquely sensitive nature of intelligence work. Specifically, neither principle addresses the national security problems that may arise as a result of whistleblowing, they simply dictate which intelligence operates are ethical and unethical. Here, De George's criteria are especially applicable. Because criteria two (2) and three (3) dictate a clear course of action for an agent to express their moral concerns about a certain action to some authority before whistleblowing, there exists the possibility for such concerns to

be addressed. This allows for all other options to be exhausted before whistleblowing must occur. Furthermore, De George's fourth (4) criterion requires that evidence exist that would convince an impartial observer that the action in question is indeed unethical. This prevents whistleblowing on trivial and ethical issues - something that would be very problematic as it may jeopardize national security with no real upside. Finally, De George's fifth (5) criterion must be modified to reflect the unique nature of intelligence whistleblowing. As aforementioned, De George considers only harm that might be done to the whistleblower if he/she decides to report some action. This criterion should be modified to consider the national security concerns of intelligence whistleblowing as well. Such an amendment may read as follows: "the employee must reasonably believe that going public will create the necessary change to protect the public and is worth the risk to oneself *and potential national security risks*."

In a similar vein, it may be apt to argue that ethical whistleblowing entails the release of only the most critical information. Whenever possible, sensitive information that is not required to reporting the unethical action should be censored. Failure to censor personal or sensitive information may increase security risks, jeopardize the well-being of some intelligence agents, and does not actively help the reporting of unethical activities. This standard, though rarely mentioned in the literature, seems to be an intuitive addition.

3.5 A New Criteria

This complete ethical framework may be summarized as follows.

Whistleblowing in the intelligence community is ethical when:

1. The intelligence operation/action is unethical.

    (a) The intelligence operation/action is carried out in such a way that the harms significantly outweigh the benefits with respect to the state's population.

(b) The intelligence operation/action is carried out in such a way that significant, disproportionate, or undue harm is caused to some individuals.

(c) Documented evidence exists that would convince a reasonable and impartial observer that the whistleblower's view of the situation is correct and significant harm would occur.

2. The intelligence agent has approached his/her direct supervisor and made his/her moral objections known.

3. Absent any action, the intelligence agent escalates his/her objections up the board as much as possible.

4. The whistleblower believes that going public will create the necessary change to protect the public and is worth the risk to oneself and potential national security risks.

5. The whistleblower takes any/all possible steps to censor, redact, or otherwise conceal any privileged information that is not absolutely necessary to reporting the unethical action.

4 Snowden as a Case Study

Few whistleblowing incidents in intelligence history have received as much press time and attention as Edward Snowden's leak of NSA surveillance program, PRISM. The controversy the event and the intricacies of the PRISM leak have earned Snowden many different titles including "whistleblower, traitor, hero, and criminal." Snowden's leak is therefore a prime case study to analyze the ethics of whistleblowing through a practical, historical lens. While this paper does not seek to explain in depth the nature of the Snowden leak, it does assume familiarity with the event.

4.1 Legal Retaliation

From a legal standpoint, Snowden's whistleblowing was illegal. Though Snowden, at the time of his leak, was working as a contractor to the CIA through Booz Allen-Hamilton (making him a covered employee under the Whistleblower Protection Act of 1989), PRISM and the documents Snowden leaked were classified (Finn and Horowitz 2013). This violates the protected disclosure clause of the Whistleblower Protection Act of 1989, as the subject matter of disclosure must "not be prohibited by law or Executive Order, except when the disclosure is made to the Special Counsel or to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosures. (Whistleblower Protection Act 1989; National Whistleblower Center 2021; Whittaker 2007)" Because Snowden chose to disclose this classified information to the press (i.e The Guardian, The Washington Post) rather than the Inspector General or head of the NSA, Snowden is not covered under the Whistleblower Protection Act of 1989. Even here, legal arguments can be made defending Snowden's actions from a legal standpoint under whistleblower legislation, though these are highly nuanced and outside the scope of this paper. Indeed, an unclassified portion of a report commissioned by the United States House Permanent Select Committee on Intelligence found that Edward Snowden was not considered a whistleblower under the Whistleblower Protection Act of 1989 (House Permanent Select Committee on Intelligence 2016).

As a result, Snowden was charged by the United States government on three felonies: (1) Theft of government property, (2) Unauthorized Communication of National Defense Information (violation of the Espionage Act), and (3) Willful Communication of Classified Intelligence Information to an Unauthorized Person (violation of the Espionage Act) (Finn and Horowitz 2013). Under the law, Snowden's whistleblowing was unethical because it did not meet the standards of contemporary whistleblower legislation. Despite this, Congress found the NSA's mass surveillance program exposed by Snowden to be illegal and unconstitutional, a decision confirmed by an appeals court in 2020 (Satter 2020).

4.2 Philosophical Analysis

From a more philosophical standpoint, it is difficult to determine whether or not Snowden's actions were ethical. From a purely utilitarian perspective, Snowden's actions were ethical. As the NSA's PRISM program was found to be both illegal and unconstitutional, Snowden's whistleblowing led to the greatest good (the shutdown of the program) for the greatest number of people (all citizens of the United States). Of course, the argument can be made that the national security violations that occurred as a result of Snowden's leak outweighed the aforementioned benefits. Insofar as the judicial system interpreted the NSA's mass surveillance program as unconstitutional (Satter 2020), though, the long-term harm of continuing such a program would likely outweigh the benefits of preserving some national security in this regard.

Using only Mills' Harm Principle, however, Snowden's actions were unethical. By exposing national security information and state secrets, Snowden hurt the security of United States citizens and eroded faith in both intelligence agencies and the government as a whole. Though Snowden's actions were done in an attempt to solve (arguably) a greater harm, they still resulted in outside individuals being harmed. Because Mills' does not make an ethical argument for harm done in the pursuit of redressing existing harm, Snowden's actions are unethical.

It is also unclear whether or not Snowden meets De George's criteria for ethical whistleblowing. Snowden did meet criterion one (1) in believing that the NSA's actions were doing serious and considerable harm to others, and criterion four (4) in having evidence that would make any reasonable and impartial observer that harm may occur. It is unclear whether Snowden met criteria two (2) and three (3), though. While Snowden argues that he brought up moral objections regarding PRISM to his supervisors, they were ignored. The government, however, maintains that they have no record of such objections (Gellmann 2013). Most importantly, Snowden does seem to meet criterion five (5) of De George's framework.

For reference, criterion five (5) is that the employee must reasonably believe that going to the public will create the necessary change to protect the public and is worth the risk to oneself. After Snowden went public with the information he had, there was widespread controversy and PRISM was eventually deemed unconstitutional. In this way, going public created the necessary change. Though Snowden has now had his passport nullified and is a permanent resident of Russia, he maintains that risking his well-being was necessary.

As above observed, however, each of these philosophical perspectives lack at least one quality that is necessary for an ethical framework with respect to intelligence whistleblowing. Analyzing Snowden's actions using the newly created criteria yields an interesting result. Firstly, it may be argued that the intelligence operation (in this case, PRISM) was unethical because it was being carried out in a way that harmed the US population (through gross privacy violations) more than it helped (through increases in national security). While this point is certainly arguable, it is within reason to find that a program deemed unconstitutional is likely net harmful. There is also documented evidence, which Snowden leaked, that would convince a reasonable and impartial observer that significant harm is being done. As mentioned above, it is unclear whether or not Snowden took his moral objections to PRISM up the ranks, with Snowden arguing that he did while the US government argues that he did not (Gellmann 2013). By the same argument made above, Snowden did believe that going public would create necessary change to protect the public and was worth the risk to his wellbeing. It is also likely that Snowden believed that leaking the information he had was worth the national security risk. Importantly, it is unclear whether or not Snowden meets the last criterion - taking all steps to censor any information not directly related to the violation. While some argue that Snowden's leaks never endangered a single life, others (particularly in the government) contend that the effects of Snowden's leaks led to small pieces of information regarding the NSA's implementation of spy infrastructure being public (Riechmann 2018). A further, more in-depth analysis is necessary to conclusively decide whether or not Snowden redacted all possible information. Likely, there will never be a

conclusive answer in this regard as much of the relevant information necessary to make such a judgment is classified.

The objective of this exercise is not to provide a conclusive answer on whether or not Snowden's actions were ethical. This paper takes no specific stance regarding his actions. Rather, this exercise is meant to demonstrate the weaknesses of current legal and philosophical frameworks by which to judge the ethics of intelligence whistleblowing. Furthermore, this exercise demonstrates the cohesive, robust framework outlined by this paper and how it may be applied to other whistleblowing case studies or be used to judge whether or not future whistleblowing instances are ethical.

5 Conclusion

Given how significant and damaging intelligence operations can be, there must be a codified framework by which potential whistleblowers can judge if whistleblowing is ethical. Currently, this framework exists as legislation established by the Whistleblower Protection Act of 1978, the Whistleblower Protection Enhancement Act of 2012, and the FISA Amendments Reauthorization Act of 2017. Problematically, this set of legislation provides vague, contradictory, and problematic ethical guidelines for whistleblowers in the intelligence industry. As such, this paper seeks to determine what such ethical guidelines should be by looking at philosophy on the subject.

While no single philosophical framework is effective at providing ethical guidelines for intelligence whistleblowing, each provides a unique and helpful point of view. Combining many of these frameworks while considering some of the nuances that exist with intelligence whistleblowing provides a strong set of criteria by which to judge whether an instance of intelligence whistleblowing was ethical.This criteria can be compared to existing criteria, laws, and philosophies through case study analyses - allowing for a comparison of its effectiveness.

This paper argues that absent a more standardized ethical framework, the one proposed here is both fair and sound.