Whistleblowing: How Millennials' Desire for Transparency Affects National Security

Rachel Gaudet

A thesis presented for the
Baker Scholar Symposium
The University of Tennessee, Knoxville

May 2016

Copyright © 2016 by Rachel Gaudet
All rights reserved.

Acknowledgements

First, I would like to thank the Baker Center and Baker Scholar Program for giving me this opportunity to perform this research and learn more about public policy through this project.

I would like to thank my Baker Scholar advisor, Dr. Joe Stainback IV, for all of his time and wisdom. Your mentorship and guidance were instrumental in not only this research project, but also in my understanding of the human element in national security.

I would also like to thank Adam Seybert, a Master's student in nuclear engineering, for his help in solidifying my direction with this project and providing assistance whenever I felt stuck; I look forward to continuing this research in future collaborations with you.

Thank you all for your help.

Abstract

Whistleblowers have long been a debated topic, are they heroes or traitors? While there will never be a unanimous decision, the act of whistleblowing itself offers many benefits when carried out through the proper channels. The very publicized Edward Snowden case offers an extreme example of the consequences that could result when a whistleblower does not follow the federal guidelines set in place. To prevent future cases like Snowden's, it becomes apparent that the current U.S. whistleblowing framework needs to be revamped and improved as more Millennials enter the workforce that could possibly possess similar ideologies to Snowden and be influenced or motivated by his dramatic plight. The purpose of the improved framework is not to prevent whistleblowing, but to prevent whistleblowing in avenues that could be detrimental to national security. Whistleblowing is a form of constant quality assurance and should be encouraged by the culture of the federal government and all associated agencies. This could support and maintain a good balance of trust between the government and its citizens – ultimately, creating a united front and strengthening national security.

List of Acronyms

CIA	Central Intelligence Agency
CSRA	Civil Service Reform Act
ICWPA	Intelligence Community Whistleblower Protection Act
MSPB	Merit Systems Protection Board
NSA	National Security Administration
OSC	Office of Special Counsel
WPA	Whistleblower Protection Act of 1989
WPEA	Whistleblower Protection Enhancement Act

Table of Contents

1. Problem Statement 1
1.1 Research Question 3
2. Introduction and Background of Whistleblowing 4
2.1 Whistleblowing Definition 4
2.2 History of Whistleblowing 4
2.3 Whistleblowing in the Age of the Internet 6
3. Edward Snowden 7
3.1 Background on Snowden 7
3.2 Snowden as a Whistleblower 8
3.3 Aftermath of Snowden's Disclosures 9
4. The Millennial Generation 12
4.1 Millennial's Characteristics and Qualities 12
4.2 Millennials in the Workplace 13
5. Current U.S. Whistleblower Framework 16
5.1 Major U.S. Whistleblowing Laws and Regulations 16
5.2 The Office of Special Counsel and Merit Systems Protection Board 18
5.3 Issues Within the OSC System 20
6. Proposal to Overcome Continued Whistleblowing Issues 22
6.1 Overview of Proposal 22
7. Conclusions 25
8. References 26

List of Figures

Figure 1. Results from survey among U.S. adults.[4]..... 2
Figure 2. Snowden's self-written bio on Twitter page. 11
Figure 3. OSC data reported in its Annual Report to Congress. 21

1. Problem Statement

In June 2013, Edward Snowden leaked thousands of classified documents to the public through journalists from the online news source The Guardian. These documents contained information regarding National Security Administration (NSA) global surveillance programs that were previously unknown to exist to the public. Snowden received access to these documents through a subcontract position with the NSA and became concerned that these surveillance programs were unconstitutional. After claiming to express his concerns about these findings to other employees and management with no result, he felt the need to release the information on a grand stage: the internet.

Although Snowden tends to paint a self-portrait of a hero -- a vigilante working for the people, his actions caused the undoing of many U.S. intelligence programs that had been collecting and building for years prior. This was followed by increased tensions between the U.S. and its allies as they felt betrayed by the information they were now discovering on the internet[1]. Overall, Snowden's actions created a hole in the U.S. national security profile, something that could continue to affect citizens for generations to come. Unfortunately, many believe what Snowden did was admirable, a view especially common among those in the Millennial generation (born 1981-2000)[2]. A survey conducted by the Pew Research Center and USA Today showed that those in the age bracket 18-29, millennials, were significantly more supportive of Snowden's leak than those in older generations. These results, shown in figure 1, can be correlated to

agree with generational studies performed that conclude Millennials are often more likely to be motivated by ideological beliefs and would prefer a more transparent government[3].

Most Young People Say Snowden's Leak Served the Public Interest

	Served public interest	Harmed public interest	Don't know
	%	%	%
Total	45	43	11=100
Men	47	44	9=100
Women	43	42	14=100
18-29	57	35	8=100
30-49	48	40	11=100
50-64	39	47	14=100
65+	35	53	12=100
College grad+	49	42	8=100
Some college	51	38	11=100
HS or less	38	48	14=100
Republican	45	43	12=100
Democrat	45	49	6=100
Independent	47	42	10=100
Among Reps/ Rep Leaners			
Tea Party	53	39	8=100
Not Tea Party	43	47	10=100
Overall view of NSA program			
Approve	43	49	8=100
Disapprove	49	41	9=100

Survey conducted Jan. 15-19, 2014.
Figures may not add to 100% because of rounding.

PEW RESEARCH CENTER/USA TODAY

Figure 1. Results from survey among U.S. adults.[4]

The fear is that it is possible Snowden's disclosures will resonate with other Millennials entering the federal workforce that might feel dissent towards information they discover through their job. If other Millennials possess the same ideological motivation

that Snowden developed, they may view his actions as laying the groundwork for this type of whistleblowing and follow in his footsteps to leak more classified information. This possibility highlights the importance of having a formal whistleblowing procedure that would be applied equally across all federal agencies. There are already offices and organizations in place to offer whistleblower protection but these are not sufficient, nor stringently regulated. The entire program needs to be revamped to create a culture where honest whistleblowing is encouraged. Not only will this ensure quality control in work produced federally, but also foster an environment where employees feel like their concerns are met with appreciation and reasonable investigation without creating a hostile relationship between the whistleblower and their respective employer. If whistleblowing internally is viewed as the better medium against Snowden's method, it will help ensure an act like his is less likely to occur in the same fashion in the future.

1.1 Research Question

How can the U.S. government improve and update procedures to encourage an internal, protected whistleblowing culture and prevent future incidents like Snowden's as more millennials enter the workforce?

2. Introduction and Background of Whistleblowing

2.1 Whistleblowing Definition

The act of whistleblowing is much like its name suggests, blowing a whistle to alert others that something has gone awry. It is commonly accepted to have been derived from English policemen who would blow their whistles to bring attention to criminal acts. Formally, a whistleblower is defined as "a person who informs on another or makes public disclosure of corruption or wrongdoing"[5].

Although a whistleblower can be part of any organization or workplace, this paper will focus on those employed by the U.S. Federal government either directly, or through subcontracting.

2.2 History of Whistleblowing

History credits Captain of Marines John Grannis as the first whistleblower. His task was simple: deliver a signed petition from his ship, Warren, that called for the removal of Commodore Hopkins, head of the Continental Navy, due to his incompetence and poor management decisions. Although Grannis' journey was arduous, the petition proved effective as the members of the Continental congress voted to relieve Hopkins of his command[6]. As this was transpiring, other crew members aboard Warren confessed their actions and signing of the petition resulting in cruel punishment and revenge from Hopkins -- this did not last long as the news of his removal finally reached him. The actions of Grannis and the other crew members not

only improved conditions in the Continental Navy, but also prompted the Continental Congress to pass the Whistleblower Law of 1778 – the first of its kind. This law reads:

> *"That it is the duty of all persons in the service of the United States, as well as all other the inhabitants thereof, to give the earliest information to Congress or other proper authority of any misconduct, frauds, or misdemeanors committed by any officers or persons in the service of these states, which may come to their knowledge." [7]*

Although records only trace back to the 1700's, it can be inferred that the practice of reporting wrongdoings of an employer, boss, or any authority figure dates as far back as the concepts themselves. Sentiments towards whistleblowers vary greatly, to some whistleblowers are heroes and to others they are villains. While there will never exist a solid, unanimous decision about which category whistleblowers fall under, much of their classification can be determined by the answers to two questions:

1. What is their motivation for whistleblowing?
2. What is their chosen method for whistleblowing?

Some studies have argued that whistleblowing is a "prosocial" behavior which involves both selfish (egoistic) and unselfish (altruistic) motives as opposed to a purely altruistic act. This means that the act of whistleblowing may not only benefit the organization, but may also benefit the whistleblower as well[8]. With the creation of the internet and its ability to distribute news and information sooner than ever before, it is very likely that a whistleblower will be given media attention very rapidly. This could be part of the egoistic motivation if the whistleblower's actions become a headline.

2.3 Whistleblowing in the Age of the Internet

Whistleblowing is no longer limited to a letter or face-to-face communication. In today's world, whistleblowers have almost infinite options for expressing their concerns. The internet provides a medium for an instant social media post, email, or anonymous tip, cell phones allow for a quick phone call, text, or video call, and transportation allows for quicker face-to-face meetings. Information sharing is no longer a process – it is an event that could only last a minute and offers the capability of reaching millions of people and leaving an impact that lasts much longer than the original whistleblowing event.

In the case of government-related whistleblowing, this ability to share information so quickly can pose an imminent threat to national security. Recent cases such as Edward Snowden and Chelsea Manning have proven that the internet is an attractive medium for leaking sensitive information in a moment. However, the effects of both cases are still being felt years later as the government must not only try to repair their reputation, but also reinstate the nation's trust in their own government. The Edward Snowden case is the main focus of this paper and offers many insights to this new approach to whistleblowing.

3. Edward Snowden

3.1 Background on Snowden

Edward Snowden, born in 1983 –thus, a millennial, grew up in Maryland with his parents who were both government employees. His mother works for the federal court in Baltimore and his father is a former officer of the Coast Guard. During a 2014 interview, Snowden stated "Everybody in my family has worked for the federal government in one way or another, I expected to pursue the same path."[9] Snowden's educational journey has been widely questioned, he dropped out of high school his sophomore year but later stated that he earned his GED. From there, his Army records show a number of classes taken at a variety of community colleges and technical schools although many of these schools have reported there was no record of Snowden as a student. In 2004, Snowden enlisted in the U.S Army Reserves but was medically discharged the same year after breaking both legs in training [10]. Snowden had other government work experience before the NSA. He worked for the Central Intelligence Agency (CIA) maintaining network security at both their headquarters in Virginia, and under a diplomatic cover in Geneva, Switzerland. Later, Snowden would express his grievances with the ethical practices of the CIA and he eventually resigned in 2009 to pursue work in the private sector. He then became a subcontractor for Dell and was first assigned to the Tokyo, Japan NSA office where he trained officials in cybersecurity and how to protect networks from Chinese hackers [9]. Investigators determined that Snowden began downloading and collecting classified documents while working for Dell

[11]. Dell reassigned Snowden to the NSA's Hawaii Regional Operations Center where he later became a subcontractor for consulting firm Booz Allen Hamilton, a position that he held for only 3 months before departing to leak the now expansive collection of classified NSA documents [12].

3.2 Snowden as a Whistleblower

On May 20th, 2013, Snowden told his supervisors he need medical leave because he had been diagnosed with epilepsy. He used this as a cover to fly to Hong Kong to meet with The Guardian journalist, Glenn Greenwald, and documentary filmmaker, Laura Poitras. Snowden contacted them using encrypted emails to remain anonymous until he was ready to meet and share his story. This was the culmination of years that Snowden spent becoming more frustrated and upset by the culture and tactics used by several government agencies. He claims that he brought his uncertainties regarding information on surveillance programs to superiors and other employees in the NSA but was met with little attention or corrective action. These claims have been disproven by internal investigations within the NSA, leading some to conclude that he bypassed the "internal channels of dissent" and went straight to the media as a whistleblower [1].

During his Hong Kong meeting, Snowden disclosed thousands of classified documents related to the NSA's surveillance programs including PRISM, a global real-time electronic information collection previously unknown to the general public [12]. Through the online news source The Guardian, the first documents were released on June 5th, 2013. This created an immediate frenzy as citizens began combing through the

leaked documents. On June 9th, 2013, Snowden emerged from the shadows and claimed responsibility for the leaks, stating "I have no intention of hiding who I am because I know I have done nothing wrong."[13]. After this revelation, the U.S. government responded with federal prosecutors charging Snowden with one count of theft of government property, and two counts of violating the Espionage Act [13]. As of May 2016, Snowden has not been arrested to appear in U.S. Court to face these charges since he has been living out of the country. In August 2014, Russia granted Snowden three more years of residency where he has been living and working ever since, though, he is rarely ever seen in public [14].

3.3 Aftermath of Snowden's Disclosures

As the documents were leaked and the public learned about the secret NSA programs, much controversy arose regarding Snowden could be considered a hero or a traitor. To some, his actions were heroic and they feel he sacrificed his life and career to prove that the U.S. government should not be fully trusted by leaking secret documents that he believed to be questionably ethical. To others, his actions appear more villainous. They see Snowden as being selfishly motivated by attention because of his choice to take his disclosures to the media instead of seeking out the proper channels in place for whistleblowers. While there will never be a clear agreement on this controversy, there is definite proof that Snowden's leak caused damage to not only U.S. intelligence programs, but to surveillance programs in the United Kingdom and Australia as well since some of the documents released discussed their efforts and plans to

support national security in their respective countries. One official familiar with Snowden's activities commented on the expanse of documents collected and leaked to the public, "This is a treasure trove of materials for any adversary of the West." [15].

The U.S. Director of National Intelligence, James Clapper, has expressed his grievances with Snowden's actions in interviews following the leaks. Clapper announced that intelligence agencies have experienced "profound damage" and "lost critical foreign intelligence collection sources, including some shared with us by valued partners" [16]. CIA Director, John Brennan, stated in the same 2014 interview that the Snowden leaks are actually aiding al Qaeda terrorists in their efforts since they can now just do a simple Google search to find what has been disclosed or leaked regarding surveillance in the middle east; this new ability has made it much tougher for the U.S. to find them and research the threats they pose [16]. The negative effects of the Snowden leak will continue to accumulate for years after the initial disclosure in the U.S. and among its allies involved in the intelligence efforts.

Even with the consequences felt around the world, Snowden has gained the status of an international celebrity. One of his main platforms is Twitter where he has accrued over 2 million followers since joining in September 2015. A 2014 study done by GlobalWebIndex concluded that 59% of millennials have a Twitter account, a number that has most likely increased in the past two years [17]. As more millennials engage on social media, the probability that more of them follow Snowden most likely also increases. This could eventually lead to more millennials being heavily influenced by his

infamous leak as they enter the workforce and begin to identify with his ideological and often biased statements and tweets. His bio on Twitter, shown in figure 2, demonstrates his marketing of himself as a public ambassador, working for the public's best interest. His tweets often follow a similar tone, usually politically charged statements or links to articles and reports on a variety of whistleblowing and government incidents.



Figure 2. Snowden's self-written bio on Twitter page.

The fear is that those being fed his opinions through social media may not also be aware of the implications and consequences of his actions. It is important that millennials are aware of the damage caused by his leaks so that future possible whistleblowers follow the federal protocol and report their concerns through the proper channels instead.

4. The Millennial Generation

It is obvious that generational qualities cannot be applied to every single person falling within that generation, however, generations do have personalities and characteristics that apply to the majority. This report focuses on these generational personalities and recognizes that these qualities are not specific to each individual.

4.1 Millennial's Characteristics and Qualities

Many studies have been done to compare and contrast the Millennial generation to those before it. It is recognized that the events and trends that occur during each generation's timeframe often play a large part in their overall disposition. For the Baby Boomer generation, born between 1946 and 1964, these events include the Civil Rights Movement, Vietnam War, and assassinations of John F. Kennedy and Martin Luther King Jr and are noted to have been raised in an era of economic prosperity. For Generation X, born between 1965 and 1980, they were raised in an era of economic uncertainty and experienced the Challenger disaster, a rise in divorce rates, and the widespread use of personal computers. Finally, for the Millennial generation, born between 1981 and 2000, it is noted that they were the first to grow up during the age of the internet and technology, and have experienced the effects of violence and terrorism including the September 11th attacks [18].

A 2010 generational study performed by the Pew Research Center focused on millennials and what distinguishes this generation from previous generations. Some chief findings from this study include that millennials:

- Embrace multiple modes of self -expression, three-fourths have created a social media profile,
- Are more ethnically and racially diverse than previous generations,
- On trend to become most educated generation in American history,
- Feel technology use distinguishes them most from other generations, and
- Are significantly more politically and socially liberal than members of other generations [19].

Overall, the main theme in defining millennials revolves around their use of the internet and its associated technology. These traits shape their relationships with other people, their approach to education, and their completion of work-related tasks.

4.2 Millennials in the Workplace

As millennial's are reaching the age and education level to enter into the professional workplace, managers and supervisors are learning that the culture of their workplace needs to be updated and tailored towards these new employees. Studies have demonstrated that millennials value transparency and clear ethical rules and expectations from their employer [3]. If they feel their needs are not being met, millennials will change jobs until they find what they are looking for as millennials are twice as likely than previous generations to want to leave within 1 year [18]. This trend should highlight the imminent need to change the balance between employer and employee to better suit the expectations of the growing number of employed millennials.

A 2009 millennials study conducted by Ethics Resource Center stated “Because they grew up in the Internet age, they value confidentiality and privacy less than other age groups. In their thinking, information flow is virtually instantaneous and knowledge is meant to be shared rather than owned.” [18] This finding could be a red flag to a bigger issue, one that could make it more difficult to prevent the spread of classified documents and information if they are employed by the federal government. The same study also determined two other ominous characteristics:

- Millennial employees are more likely to find it acceptable to blog or tweet negatively about their company, and
- They are more likely to find it acceptable to keep copies of confidential documents. [18]

Other researchers have found that this cohort grew up in an age where seemingly no behavior goes unnoticed or unreported due to increased governmental regulation, 24-hour news sources, increased reporting of large-scale ethics violations, and the pervasiveness of social media. These phenomena have resulted in the fact that millennial idealists are less tolerant of ethical violations [2].

Unfortunately, these characteristics are reminiscent of the Snowden incident motivations and bring fear that this type of incident is more prone to occurring as more millennials reach employment level. This fear of possible repeating incidents highlights the importance of maintaining a balanced culture of transparency and rigorous ethical guidelines and rules. Grey areas existing in rules and procedures lead to more

misunderstandings and violations of the employer code of conduct. In the case of an employee finding themselves displeased or concerned with their employer's ethical behavior or work in the field, guidelines for reporting these concerns need to be clear and well-advertised by the employer. Snowden's leaks emphasized a problem within the current U.S. whistleblower framework. To prevent future incidents like his, the federal whistleblower system needs to be more robust and comprehensive.

5. Current U.S. Whistleblower Framework

There are many federal and state laws that acknowledge whistleblowing in some manner. However, there are four major federal laws that directly affect whistleblowers in U.S. government agencies. These laws build upon each other to create the current whistleblower framework.

5.1 Major U.S. Whistleblowing Laws and Regulations

The Civil Service Reform Act (CSRA)

Passed by Congress in 1978, this Act, among other goals, sought to recognize whistleblowers and protect those that disclosed information that they believed provided evidence of a violation of a law, rule, or regulation [20]. The Act also created the Office of Special Counsel (OSC) which would examine the disclosures of the whistleblower, investigate the possible wrongdoings for legitimacy, and advocate for whistleblower protection. These claims could be pursued before the United States Merit Systems Protection Board (MSPB), a type of administration court, either to defend an appealable personnel action or an action presented on behalf of the whistleblower by the OSC [20].

The Whistleblower Protection Act of 1989 (WPA)

This Act addressed some of the weaknesses found in the whistleblower provisions from the Civil Service Reform Act. In order to receive the provisions under the WPA, a case must contain: a personnel action taken because of a protected disclosure, made by a covered employee [21]. It is important to distinguish that anyone may

disclose information as a whistleblower for referral to their appropriate agency, however, an investigation and report from that agency head is required only if the information is received from a "covered employee". Most federal employees are covered, but there are some exclusions such as those employed by the U.S. Postal Service, Government Accountability Office, and many of the Intelligence Community Agencies.

The Whistleblower Protection Enhancement Act (WPEA)

The WPA is known to have many flaws that result in whistleblowers not being protected the way it was intended to work. The WPEA, signed by President Obama and enacted in 2012, was created to close some of the court created loopholes and better protect whistleblowers from reprisal. This Act also extended the protection to all Transportation Security Agency employees. Under the WPEA, the MSPB was given further authorization to award compensatory damages to whistleblowers to help offset legal fees and associated costs and works to ensure due process rights at MSPB hearings. Ultimately, the WPEA was intended to "fix" issues with the WPA by strengthening protection of whistleblowers and ensures all employees are well-versed in their whistleblowing protocol through their broad outreach effort.

The Intelligence Community Whistleblower Protection Act (ICWPA)

As previously mentioned, most intelligence agency employees are not covered by the WPA. The ICPWA of 1998 was created to provide a secure means for employees to report allegations of wrongdoing to Congress. The agencies that fall under the ICWPA

are: Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and the National Security Agency; the Department of Defense Office of Inspector General was implemented into the ICWPA in 2007. The ICWPA does not grant special protections to whistleblowers in the intelligence community, instead it sets the procedural approach if employees wish to file a complaint that may contain classified information. Other intelligence agencies such as the Federal Bureau of Investigation and the Central Intelligence Agency have their own, agency specific, rules and guidelines in place.

5.2 The Office of Special Counsel and Merit Systems Protection Board

The OSC is responsible for handling claims of wrongdoing within the executive branch of the federal government. Current, former, and applicants for federal employment within the agencies for which the OSC covers are allowed to submit disclosures. The OSC's Disclosure Unit is responsible for handling this process and can review five types of disclosures as specified in their statute:

1. Violation of a law, rule, or regulation,
2. Gross mismanagement,
3. A gross waste of funds,
4. An abuse of authority, and/or
5. A substantial and specific danger to public health or safety [22].

Employers can use their online form, fax, or mail to submit their disclosure. Once the disclosure is received, OSC interviews the federal employee by phone and continue to

evaluate all information provided. If it is determined that there is a substantial likelihood that the information in the disclosure provides evidence that one of the 5 types of disclosures is met, the case is then referred to the appropriate agency head who is required to investigate. If the investigation reveals evidence of a criminal violation, the report will be sent to the Office of Personnel Management. However, in most cases, the report is sent back to the whistleblower for review. The OSC can then decide if the findings appear "reasonable" and the process is complete after finally being sent to the President and congressional committees with oversight responsibility [22]. The identity of the whistleblower is not revealed to OSC without their consent, except if the Special Counsel determines the case suggests an imminent danger to public health, safety, or violation of criminal law which the identity may then be revealed.

While it is the OSC's responsibility to investigate allegations of prohibited personnel practices brought up by individual whistleblowers, they may involve the MSPB if the OSC is unable to obtain a satisfactory correction of the practice from the agency in which the investigation was carried out. Described as an independent, quasi-judicial agency in the Executive branch that serves as the guardian of Federal merit systems, the MSPB hears appeals from employees that were subjected to an adverse personnel action as a result of that employee engaging in whistleblowing. Their main focus is protecting individuals after a whistleblowing disclosure was made to ensure they are not subject to retaliation or reprisal.

5.3 Issues Within the OSC System

Although the WPEA has worked to prevent issues within the OSC and MSPB that work against whistleblowers, there are still concerns over their practices today. The information in OSC's fiscal year 2014 Report to Congress demonstrated that the number of submitted disclosures is on the rise. The table shown in figure 3, is taken directly from this report and details the submissions per fiscal year. For FY 2014, there were 1,747 total disclosures, however, only 92 of these disclosures were referred to agency heads for investigation [23]. This figure could be alarming to possible whistleblowers that feel discouraged to submit their concerns, they may feel like the hassle and effort to submit the disclosure is not worth it if only 5% of the disclosures get investigated by agency heads. This could point to a possible internal issue within the OSC general framework and processes and should notify lawmakers that there is still room for improvement in the whistleblower procedures.

Table 7 below contains FY 2014 summary data (with comparative data for the six previous fiscal years) on the receipt and disposition of whistleblower disclosure cases.

TABLE 7 Summary of Whistleblower Disclosure Activity – Receipts and Dispositions[a]

		FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013	FY 2014
Pending disclosures carried over from prior fiscal year		84	128	125	83	132	225	193
New disclosures received		530	724	961	928	1,148	1,129	1,554[b]
Total disclosures		614	852	1,086	1,011	1,280	1,354	1,747
Disclosures referred to agency heads for investigation and report		40	46	24	47	39	51	92
Referrals to agency IGs		9	10	2	5	6	2	0
Agency head reports sent to President and Congress		25	34	67	22	36	54	26
Results of agency investigations and reports	Disclosures substantiated in whole or in part	22	30	62	21	31	49	25
	Disclosures unsubstantiated	3	4	5	1	5	5	1
Disclosure processing times	Within 15 days	256	394	555	555	583	575	731
	Over 15 days	232	333	451	315	470	585	584
Percentage of disclosures processed within 15 days		52%	54%	55%	63%	55%	49%	55%
Disclosures processed and closed		488	727	1,006	870	1,053	1,160	1,315

Figure 3. OSC data reported in its Annual Report to Congress.

6. Proposal to Overcome Continued Whistleblowing Issues

This section will focus on the ideas that make up my own proposal for strengthening the federal whistleblower framework in the U.S. While the system should be strengthened for all employees, it is important to note that more millennials are joining the federal workforce as the previous generation employees are reaching the age of retirement. For these reasons, much of this proposal is catered towards satisfying the needs and desires millennials have for their employers as discussed in section 4.

6.1 Overview of Proposal

Whistleblowing at a basic level is simply the reporting of perceived wrongdoing in a place of employment and in the altruistic sense offers many benefits. To receive these benefits, the workplace must maintain a culture conducive to proper whistleblowing. The culture of the agency must highlight ethical, law-abiding behavior and employees must feel that management not only encourages, but requires employees to report any observances that do not follow this culture. This means that other employees must not view the whistleblower as a “snitch” or enemy of their agency, but recognize that they are trying to improve the work and increase accountability.

Since the OSC already has much of the framework in place, it would be most efficient for the improvements to be applied to their existing procedures and infrastructure. The online disclosure form would cater most to the technology savvy millennial generation so simplifications and routine maintenance should be done on the

website to ensure it is available for use. The online form with the ability to be submitted anonymously is the best option that may deter spurious or unmerited claims since it requires more effort than calling a hotline in a desperate moment of frustrated revenge.

To possibly address and curb the issue of only 5% of OSC submitted disclosures being sent to agency heads for investigation, an independent party should be brought in for verified investigations within the agencies. This third-party investigator would be given full legal rights and jurisdiction to carry out their duties. The current framework calls for agencies to do their own internal investigations which could be leading to more wrongdoing or corruption if they are trying to cover up the actions reported by the whistleblower. Employees may also feel more inclined to submit disclosures if they recognize that their report will be anonymous and investigated by a party outside of their respective agency that will then report their findings back to the whistleblower for review before submitting it to the OSC.

To hopefully prevent more incidents like Snowden's leak to the media and general public, the OSC and its offerings for whistleblowers should be heavily advertised. All newly hired federal employees should be formally introduced to the OSC through their required training modules. Subsequent advertisement should follow the initial introduction to refresh employees' memory that the office exists and offers assistance in whistleblowing cases.

To assure employees that their disclosures are valuable to the well-being of federal agencies, a reward should be offered for legitimate whistleblowing disclosures

that result in a corrective action after the investigation. The reward could be monetary or paid time off. In these cases, the whistleblower's identity would need to be revealed with their permission. Often, whistleblowers are hesitant to step forward with their information because they feel like it could be detrimental to their career. With the combination of third-party administered protection and a reward, whistleblowers should view those concerns as less of a barrier.

Much like the investigation of disclosures to OSC, the appeals to MSPB for whistleblowers who believe they have been the target of reprisal or retaliation should also be investigated by a third party. The cliché "who's checking the checker" is commonly used to remind others that there should always be a valid form of checks and balances. In this case, the checker should not be checking themselves or their own agency as is currently practiced. The independent party should also have jurisdiction to determine if these claims are legitimate.

To summarize, the proposal calls for a third party to be brought in as a tool for the OSC to carry out their investigative and protective actions. This eliminates the step of the OSC referring their cases to agency heads to then be investigated internally. The whistleblower should still be an active participant in the final review of the case after the investigation has concluded and should be rewarded for their actions in voicing their concerns. The majority of the administrative details in the current framework would remain, including the online disclosure forms.

7. Conclusions

The purpose of this report is not to prevent whistleblowing in general, but to prevent whistleblowing in avenues that involve leaking classified information to the general public. This task can be accomplished by improving current federal framework and creating a more robust whistleblower policy and program. The current framework under the OSC and MSPB offers the perfect opportunity to use what is already in place, and just build in the areas that need improvement. The hope is that these proposed changes could prevent future whistleblowers from taking the same route Snowden took when he chose to leak millions of classified NSA documents that he felt represented violations of ethical conduct. It is important that new employees, especially those in the same generation as Snowden, the Millennial generation, recognize that there are other options for whistleblowing that do not require breaking federal laws. Millennials are known for sharing their thoughts and concerns, their workplace should be no different.

Whistleblowing is an integral part of the federal government and should be encouraged because it translates to constant quality assurance provided by those on the front lines of their work as opposed to a short-term audit that may miss some of the underlying issues. Quality assurance contributes to maintaining a good reputation with the general public, something that is extremely valuable in an age where all information is shared rapidly across the internet. Ultimately, whistleblowing leads to a nation where the government is trusted and respected by its citizens, this quality shows a united front to other nations and strengthens national security.

8. References

1. Gellman, B., *Edward Snowden, after months of NSA revelations, says his mission's accomplished*, in *The Washington Post*. 2013.
2. Van Meter, R.e.a., *Generation Y's Ethical Ideology and Its Potential Workplace Implications.* Journal of Business Ethics, 2012(117): p. 93-109.
3. Curtin, P.e.a., *Millennials' Approaches to Ethical Decision Making: A Survey of Young Public Relations Agency Employees.* Public Relations Journal, 2011. **5**(2).
4. Union, A.C.L., *ACLU Edward Snowden Survey*. 2015, KRC Research.
5. Dictionary.com, *The Random House Dictionary*. 2016, Random House, Inc.
6. Boisson, S., *The First Whistleblowers*, in *American History*. 2015.
7. Congress, C., *Journals of the Continental Congress*. 1778.
8. Dozier, J.M., Marcia, *Potential Predictors of Whistle-blowing: A Prosocial Behavior Perspective.* The Academy of Management Review, 1985. **10**(4): p. 823-836.
9. Bamford, J. *Edward Snowden: The untold story of the most wanted man in the world*. 2014.
10. Mosk, M.e.a. *TIMELINE: Edward Snowden's Life As We Know It*. 2013; Available from: http://abcnews.go.com/Blotter/us-fears-edward-snowden-defect-china-sources/story?id=19389672.
11. Hosenball, M. *Snowden downloaded NSA secrets while working for Dell, sources say*. 2013.

12. Editors, B.c. *Edward Snowden Biography*. Available from: http://www.biography.com/people/edward-snowden-21262897.

13. Greenwald, G.e.a. *Edward Snowden: the whistleblower behind the NSA surveillance revelations*. 2013.

14. Gorst, I. *Russia gives Edward Snowden asylum for three more years*. 2014.

15. Coughlin, C. *Our enemies are stronger because of Edward Snowden's treacherous betrayal*. 2014.

16. Meek, J.G.e.a. *Intel Heads: Edward Snowden Did 'Profound Damage' to U.S. Security*. 2014.

17. Index, G.W., *Generations Audience Report: Q2 2014*. 2014.

18. Center, E.R., *Millennials, Gen X and Baby Boomers: Who's Working at Your Company and What Do They Think About Ethics?* 2009.

19. Keeter, T., *A Portrait of Generation Next.* 2010.

20. Vaughn, R.G., *Whistleblower Protection and the Challenge to Public Employment Law*, in *Public Sector Employment in the Twenty-First Century*. 2007, Australian National University: Canberra.

21. Shimabukuro, J.O.W., L. Paige, *Whistleblower Protections Under Federal Law: An Overview*, in *CRS Report for Congress*. 2012, Congressional Research Service.

22. Counsel, O.o.S. *Disclosure of Wrongdoing Overview*. Available from: https://osc.gov/Pages/DOW.aspx.

23. *Annual Report to Congress for Fiscal Year 2014*. 2014, U.S. Office of Special Counsel: Washington, D.C.