The Case of Edward Snowden
A Different Path

Introduction

Legitimate whistleblower or traitor? While the public continues to debate which of these titles most aptly describes former National Security Agency (NSA) employee Edward Snowden, a movie set to start filming in January 2015 attests to the continuing fascination with the man at the center of the controversy. Some consider his revelations “courageous” and call for granting him asylum, but an increasing number of Americans, as many as 60 percent in a late 2013 ABC News poll, view his unauthorized disclosures as damaging to US security, a jump of 11 percent within a year. Unsurprisingly, the vast majority of respondents who believe Snowden harmed US security interests also believe he should be punished; however, public opinion on the whole has been divided along an almost even split as to whether Snowden should face such prosecution. Despite this split, the fact remains that he leaked classified information by circumventing the protected whistleblowing structure within the Intelligence Community (IC). Well aware of his contractual obligations, Snowden still decided to disclose evidence, in an unauthorized and very public way, indicting Snowden still decided to disclose evidence, in an unauthorized and very public way, indicting

Law enforcement response is to be used to the injury of the United States, to whistleblowers, like Snowden, within such institutions.

The paper proceeds with an overview of the history of legislation and case law regarding whistleblowing in the IC. Analysis of three separate whistleblowing cases follows, illuminating the contemporary legal protections afforded to such whistleblowers. The final section consists of the argument that Edward Snowden, the most recent high-profile whistleblower, is fully culpable, in the legal sense, for his actions given the recourses he decided to ignore.

Historical Background

After the government scandals of the 1970s and 1980s, like the Watergate break-in and cover up and the Iran-Contra scandal, trust between the government and the public reached a nadir, causing Congress to call for investigative commissions and to pass several pieces of legislation intended to enhance government accountability and transparency. These reforms included explicit protections for whistleblowers, defined as those federal employees who “[make] a disclosure evidencing illegal or improper government activities.” However, most of the subsequently passed pieces of legislation included exceptions for agencies, like the Central Intelligence Agency (CIA) and NSA, that make up the Intelligence Community. Employees within this special community are subject to signing non-disclosure agreements, and can be threatened with job termination, security clearance revocation, fines, and time in prison should they be found guilty of disclosing sensitive information in an unauthorized way.

Legislation and Case Law

One statute used to inflict such punishment, the Espionage Act of 1917, prohibits those entrusted with national security secrets “with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation,” from taking and communicating information related to national defense. The statute also includes clauses that could be used to prosecute those who publish such information, but no such charges have arisen in recent cases. Furthermore, whistleblowers can suffer from retaliatory actions and personal consequences because of their decision to raise concerns.

In addition to these threats, potential whistleblowers in the IC must contend with a recent Supreme Court decision that limited the opportunities for them to voice their concerns. In Garcetti v. Ceballos, the Supreme Court ruled, “When public employees make statements pursuant to their official duties, they are not speaking as citizens for First Amendment purposes, and the Constitution does not insulate their communications from employer discipline.” When applied to members of the Intelligence Community, employers can argue that keeping national security secrets is a part of these official duties, preventing whistleblowers within the IC from stepping forward under protection provided by the First Amendment. Instead, the venues and protection available to whistleblowers, like Snowden, within such agencies stem from the offices of Inspectors General, Congressional legislation, and recently, a presidential directive.

The Office of Inspector General provides the most robust legitimate outlet for public employee concerns and dissent about programs within the Intelligence Community. Currently, “every significant federal agency charged with national security responsibilities...has an inspector general,” who is generally charged with acting as an oversight mechanism for the secretive IC, but these offices differ in their statutory or Agency-appointed origins. The aptly named Inspector General Act of 1978 created...
thirteen statutory Inspector Generals (IGs) for executive departments, but excluded the CIA, which had a non-statutory IG, from needing one. However, after the Iran-Contra scandal came to light, Congressional reports contended that the non-statutory office lacked enough power to provide proper oversight, and on December 30th, 1989, the position became statutory. The NSA Inspector General, in contrast, remained an Agency-appointed position, resembling the CIA inspector of old rather than enjoying status as presidentially-appointed, until this year. In the most recent Intelligence Authorization Act, which was signed into law on July 7th, 2014, Congress made the IGs for both the National Reconnaissance Organization (NRO) and the NSA statutory positions.

Mirroring the purposes given for other IG offices, the statutory CIA IG was established to “create an objective and effective office, appropriately accountable to Congress, to initiate and conduct independently inspections, investigations, and audits relating to programs and operations of the Agency, [and to] detect fraud and abuse in such programs and operations…” The legislation empowers employees with “urgent concerns” about Agency activities to submit such concerns to the Inspector General, or to the Congressional Intelligence Oversight Committees directly under certain conditions and protects such employees from punitive action if the concerns were raised in good faith. The IG must determine if the concerns merit further action, and within a short time frame relay “particularly serious or flagrant” problems to the Director of Central Intelligence (DCI) who must in turn report the concerns to the Congressional intelligence committees. However, the act also includes a provision permitting the DCI to prohibit the IG from investigating concerns if such a ban is deemed “necessary to protect vital national security interests of the United States.”

While the powers enjoyed by the offices of Inspectors General render them “the most powerful and feared internal government watcher,” Congress deemed more explicit protection for whistleblowers necessary because employees did not feel adequately protected from reprisals. According to an overview of the Intelligence Community Whistleblower Protection Act (ICWPA) of 1998, “the risk of reprisal perceived by employees and contractors of the Intelligence Community for reporting serious or flagrant problems to Congress may have impaired the flow of information needed by the intelligence committees to carry out oversight responsibilities.” Protection for whistleblowing federal employees did exist through the Whistleblowing Protection Act (WPA) of 1989, but it explicitly exempted employees within the Intelligence Community from its protection. Accordingly, Congress passed the ICWPA with the rationale that “an additional procedural should be established that provides a means for such employees and contractors to report to Congress while safeguarding the classified information involved in such reporting.” However, a former federal field solicitor, Robert J. McCarthy, noted that the act “does not actually protect whistleblowers against reprisal. Instead, it simply authorizes employees of intelligence agencies to bring matters of ‘urgent concern’ to congressional attention through the Office of Inspector General…any disclosure to someone other than the IG would be illegal under the Espionage Act of 1917, 18 U.S.C. §§ 793–799.”

In light of the number of high profile leaks in recent years, Congress has attempted to overcome the gaps in protection extended to members of the Intelligence Community because enhanced protection ensures that concerns flow through legitimate channels. The Whistleblower Protection Enhancement Act of 2012 actually increases the number of agencies excluded from the original legislation, but it protects employees if they “are not the first person to disclose misconduct; disclose misconduct to coworkers or supervisors; disclose the consequences of a policy decision; or blow the whistle while carrying out their job duties.” A recently submitted bill, the Intelligence Authorization Act for Fiscal Year 2014, mandates that no employee should suffer adverse consequences for bringing a concern to the attention of the appropriate directors, IGs, or congressional intelligence committee members. Powers exercised by the Executive Branch mirror this concern with protecting IC employees. In 2007, President Obama sign Presidential Directive 19, which forbade practices like firing whistleblowers for their authorized disclosures, presented an IG panel as an alternative method of disclosure, and mandated the establishment of remedies like compensation for employees subjected to such retaliatory action, with other stipulations focusing on implementing WPA-like procedures within the IC.

However, in conjunction with this move to protect whistleblowers, the Obama Administration has taken an unprecedentedly tough stand against national security leaks. In just 17 months, the President outstripped every previous president in investigating and seeking redress against leakers, and while he professes admiration for whistleblowers in general, he promised an aggressive pursuit of leakers involved in national security matters. Despite the aggressive stance, the success rate of such prosecutions has been minimal, particularly as compared with the number of leaks that
remain unpunished because the associated court proceedings may reveal even more classified information and are often politically controversial. Furthermore, as demonstrated by the Administration’s insistence on using the Espionage Act of 1917 to bring many of its charges, “the relevant laws are old and vague, making prosecution difficult.”

**Case Comparisons**

Despite these shortcomings, the government has charged several employees within the Intelligence Community with making unauthorized disclosures over the years, including Frank Snepp, Thomas Drake, and most recently, Edward Snowden. In each of these three cases, the employee eschewed the authorized methods of disclosure, albeit for differing reasons, and suffered for their decisions, both professionally and personally. Furthermore, these public servants were not working for a foreign power but rather, at least ostensibly, made their disclosures with the aim of educating the public about failures within the IC. Both Frank Snepp and Thomas Drake suffered the consequences of their decisions to go public outside of the authorized structure, but the question remains as to what will happen to Snowden.

**Frank Snepp: Unclassified but Unauthorized**

The case of Frank Snepp represents the consequences members of the IC face when they violate their contractual employment obligations by circumventing the information dissemination process, but without disclosing any real national secrets. Snepp was a CIA officer active during the Fall of Saigon who quit the Agency and decided to write a book about the events that occurred then and the intelligence failures that led to them. Upon entering the Agency, he signed an agreement that he would not disclose classified information in an unauthorized manner or publish any information without submitting it to the Agency’s prepublication review board. However, he published his book, Decent Interval, without conforming to the Agency’s review process, purportedly because the Department of Justice on behalf of the CIA. In Snepp v. United States, the Supreme Court ruled that Snepp had violated the trust bestowed on him by the CIA as indicated in his employment contract.

In Snepp v. United States, the Supreme Court ruled that Snepp had violated the trust bestowed on him by the CIA as indicated in his employment contract. Despite the fact that his book did not disclose classified information, the Agency believed and the courts ruled that “a former intelligence agent’s publication of unreviewed material relating to intelligence activities can be detrimental to vital national interests even if the published information is unclassified,” citing foreign intelligence sources who ceased cooperating with the CIA out of concern for the Agency’s ability to keep secrets. Accordingly, the Court ordered that Frank Snepp be stripped of the proceeds from Decent Interval, which would be put into a constructive trust, and that he be forced to submit all publications, barring cookbooks or garden works, to the CIA’s prepublication review process. Snepp contends that he received such a sentence because the CIA “set out to chill all potential whistle-blowers by seeking severe penalties against [Snepp] without any proof of damage to anybody.” However, the fact remains that Snepp violated his employment agreement and suffered the proscribed consequence because he did not attempt to use the Agency’s authorized methods of disclosure before informing the public of unclassified information.

**Thomas Drake: “The Nuclear Option”**

On the other hand, the government charged Thomas Drake with retaining classified information and leaking it to a reporter. Despite the fact that his book did not put his name on the complaint, he allegedly served as a source to Diane Roark, an aide on the House Intelligence Committee, who shared his concerns about government wastefulness. Their concerns centered on Drake’s favored NSA project, ThinThread, which was scrapped for an apparently less effective and more expensive program. Drake also raised concerns about the NSA’s alleged abandonment of constitutional safeguards against collecting information on innocent Americans without a warrant. He reportedly mentioned his concerns about the constitutionality of the NSA program to his boss and the NSA’s general counsel while Roark attempted to contact Supreme Court Justice Rehnquist through informal channels, but Drake never explicitly filed a report for the Inspector General related to this concern about constitutionality. Developers of the ThinThread program filed a complaint about government wastefulness with the Pentagon’s Inspector General in September of 2002, and although Drake did not put his name on the complaint, he allegedly served as a key source of information. The resulting IG report was classified as secret, but one news source contends that it spawned two criminal fraud inquiries despite the fact that Drake never saw an impactful response to the complaints. In 2007, FBI agents raided the

---

**Frank Snepp: Unclassified but Unauthorized**

The case of Frank Snepp represents the consequences members of the IC face when they violate their contractual employment obligations by circumventing the information dissemination process, but without disclosing any real national secrets. Snepp was a CIA officer active during the Fall of Saigon who quit the Agency and decided to write a book about the events that occurred then and the intelligence failures that led to them. Upon entering the Agency, he signed an agreement that he would not disclose classified information in an unauthorized manner or publish any information without submitting it to the Agency’s prepublication review board. However, he published his book, Decent Interval, without conforming to the Agency’s review process, purportedly because the Department of Justice on behalf of the CIA.

In Snepp v. United States, the Supreme Court ruled that Snepp had violated the trust bestowed on him by the CIA as indicated in his employment contract. Despite the fact that his book did not disclose classified information, the Agency believed and the courts ruled that “a former intelligence agent’s publication of unreviewed material relating to intelligence activities can be detrimental to vital national interests even if the published information is unclassified,” citing foreign intelligence sources who ceased cooperating with the CIA out of concern for the Agency’s ability to keep secrets. Accordingly, the Court ordered that Frank Snepp be stripped of the proceeds from Decent Interval, which would be put into a constructive trust, and that he be forced to submit all publications, barring cookbooks or garden works, to the CIA’s prepublication review process. Snepp contends that he received such a sentence because the CIA “set out to chill all potential whistle-blowers by seeking severe penalties against [Snepp] without any proof of damage to anybody.” However, the fact remains that Snepp violated his employment agreement and suffered the proscribed consequence because he did not attempt to use the Agency’s authorized methods of disclosure before informing the public of unclassified information.

**Thomas Drake: “The Nuclear Option”**

On the other hand, the government charged Thomas Drake with retaining classified information and leaking it to a reporter. Despite the fact that his book did not put his name on the complaint, he allegedly served as a source to Diane Roark, an aide on the House Intelligence Committee, who shared his concerns about government wastefulness. Their concerns centered on Drake’s favored NSA project, ThinThread, which was scrapped for an apparently less effective and more expensive program. Drake also raised concerns about the NSA’s alleged abandonment of constitutional safeguards against collecting information on innocent Americans without a warrant. He reportedly mentioned his concerns about the constitutionality of the NSA program to his boss and the NSA’s general counsel while Roark attempted to contact Supreme Court Justice Rehnquist through informal channels, but Drake never explicitly filed a report for the Inspector General related to this concern about constitutionality. Developers of the ThinThread program filed a complaint about government wastefulness with the Pentagon’s Inspector General in September of 2002, and although Drake did not put his name on the complaint, he allegedly served as a key source of information. The resulting IG report was classified as secret, but one news source contends that it spawned two criminal fraud inquiries despite the fact that Drake never saw an impactful response to the complaints. In 2007, FBI agents raided the...
homes of the three developers, along with Roark and Drake, and in Drake’s case the investigation culminated with the charge that he violated the Espionage Act and could be sentenced to up to 35 years in prison. The other developers and Roark have never faced charges in connection with the incident.

Some contend that the Drake case and its associated investigations represent attempts to repress whistleblowers in the IC, but the final outcome may point to a victory for whistleblowing. Because of their signatures on the IG report, the program developers, “became targets…[in] ‘the most severe form of whistleblower retaliation’” one activist had ever seen. Another news report argues that Drake “first tried the sanctioned methods -- going to his superiors, inspectors general, Congress. Finally, in frustration, he turned to the ‘nuclear option’: leaking to the media.” However, this latter account omits the key details that Drake never initiated an IG complaint about the warrantless data acquisitions, only indirectly participated in an IG report about government waste which spawned action, and did not raise his concerns to Congress through the protected methods of disclosure, choosing instead to rely on a congressional aide to go through indirect channels. Drake argues that he had to use these unauthorized methods of disclosure because the formal channels of complaint were not as impactful as they should be, but others think he was just a disgruntled Washington bureaucrat who endangered national security when he did not get his way. Whatever his real motives were, the government dropped all charges against Drake except a misdemeanor for exceeding the authorized use of a government computer, he was sentenced to one year of probation and 240 hours of community service. The government’s case against him “collapsed” because the NSA refused to divulge compromising details about its programs for an investigation and the pieces of information recovered from his possession were either unclassified or quickly declassified, leading to what one pro-whistleblowing activist called “a victory for national security whistle-blowers.” Moreover, as he decided to leak beginning in 2006, his frustration with the system preceded, and probably inspired, the most recent reforms introduced by Presidential Directive 19 of 2007 and the WPEA of 2012.

Edward Snowden: The Current Spotlight

Against this backdrop, the Edward Snowden situation remains a sore spot, both for the Intelligence Community and the broader Obama Administration. Snowden was a contractor working for the NSA who took top-secret information from his work and fled the country, releasing the information to reporters around the world. Drake contends that his experience with perceived persecution within the NSA may have influenced Snowden’s decision to run straight to the press, but the parallel omits the fact that Snowden, in a strictly legal sense, could have enjoyed the protections added by the Presidential Directive 19 and the WPEA. Unlike the other two cases, however, there is no doubt that the information revealed by Snowden was highly classified and its release gravely harmed American interests, the Intelligence Community in particular, and interstate relations. As of June 2013, the Department of Justice charged Snowden with three felonies, each carrying a penalty of as many as 10 years in prison, for “conveying classified information to an unauthorized party, disclosing communications intelligence information, and theft of government property.” However, he reportedly remains in Moscow, Russia, asking the international community to help persuade the US to drop spying charges against him. With important public debate stemming from his disclosures and some heralding his efforts as heroic, Edward Snowden represents an area of ambiguity in the traitor-hero dichotomy in the minds of many. He shed light on NSA programs that have many Americans calling for reforms, even leading Secretary of State John Kerry to say, “some NSA spying went too far.” However, he bluntly violated the terms of his security clearance and employment contract, applicable even though he served as a contractor, and severely undercut US national security interests, while never attempting to channel his dissent through unauthorized whistleblower structures like the IGs or Congress before jetting off in a dramatic attempt to seek asylum abroad.

In the world of shadows populated by the Intelligence Community, the question arises if the public would have ever known about the extent of the NSA programs had Snowden followed protocol. While the public debate has been constructive, the way in which it was brought about has not been as salutary. As one leader in the intelligence community speaking about the CIA testified to Congress, “The issue is really perceptions. And if our intelligence assets around the world, particularly cooperating intelligence organizations, perceive that the CIA has no control over the information which is given it…the intelligence assets will dry up.” As this testimony reveals, the IC must protect its secrets to do its job, and leakers like Snowden can catastrophically undercut the US ability to protect its interests.

In fact, members of the House Intelligence Committee described a classified Pentagon report that revealed Snowden’s
disclosures damaged U.S. efforts “not just against terrorism, but cybercrime, human trafficking, and weapons proliferation.”74 Because, as one description of the report notes, “Most of the estimated 1.7 million classified documents that Snowden copied from NSA computers involve U.S. military operations,” his disclosures will cost the U.S. government billions of dollars to mitigate the damages done to those operations according to the chairman of the House Intelligence Committee.75 Others put the number of documents he leaked closer to the thousands, but either way Snowden leaked massive amounts of information that did not relate to his concerns about NSA surveillance on Americans. Fred Kaplan, after reviewing a documentary about Snowden, writes, “Judging from Snowden-derived stories in The Guardian and The Washington Post, some of these documents also detail NSA intercepts of email and cellphone conversations by Taliban fighters in Pakistan; assessments of CIA assets in several foreign countries” among other things.76 A story by the National Public Radio’s All Things Considered program reveals that divulging such information might have led terrorists to change their communication tactics, much like Osama Bin Laden did after he learned the IC was tracking him.78 With these costs in mind, the whistleblowing structure afforded Snowden another path for disclosure, one that would have certainly been less costly to American security interests.

If Snowden brought his concerns, which certainly warranted even more attention than the bureaucratically charged issues highlighted by the IG report related to the Drake case, to the Inspector General, the IG would have had to follow protocol and investigate. George Ellard, the NSA’s Inspector General, argues that such an investigation would have shown that the NSA was within the parameters of the law.79 However, Snowden could also have reported his concerns directly to the Congressional intelligence committees who then should have exposed the alleged abuses properly, and addressed them, without gratuitously undermining US security.

Certainly, the possibility always exists that the authorized channels could fail to address fully the concerns of a whistleblower. Drake contends that his case provides an example of such a failure of whistleblowing channels to bring real attention to a problem. However, earlier this year, Ellard publicly stated that the NSA’s complaints hotline receives an estimated 1,000 submissions per year and that “[the NSA] has surprising success in resolving the complaints that are brought…”76 Ellard is far from an unbiased source, but his insights shed light on the existence of an active whistleblowing structure. Perhaps using the authorized channels, first the NSA IG and then the Congressional committees, would not have engendered the rich public discussion about the balance between privacy and security. Furthermore, as the recent move to make the NSA IG a statutory position shows, the whistleblowing structure has been strengthened in the wake of Snowden’s disclosures. However, Snowden did not even try to disclose his concerns through the very channels designed to handle this type of issue, and that is where many qualms about his actions lie.

At the present, the Obama Administration will be under pressure to sew up the festering Snowden case. To many, allowing Snowden to walk away freely risks causing ever more leaks to spring as potential whistleblowers follow Snowden’s example of running straight to the press and those seeking to garner similar levels of global fame witness a light sentence for international recognition. The sheer amount of information made public by Snowden should overcome any concerns that more details must be revealed to prosecute him; enough information is probably already out in the open to sustain an investigation. The Administration’s position that Snowden must return to the United States and face trial remained unchanged earlier this year.79 Snowden sealed his own fate when he decided to eschew the legislative and presidential protections for whistleblowers by disclosing highly classified information. These protections for whistleblowers exist, and while they could function imperfectly at times, they at the very least deserve a chance to work. Whatever its previous failures, the whistleblowing structure would have insulated Snowden from prison time and would have saved him from self-imposed exile.

While the whistleblower protection structures have only grown in fits and starts through legislation and presidential directive, such protection does exist and could have been used by Edward Snowden. Employees within the IC were largely excluded from the protections afforded by the WPA and the later ICWPA has been deemed largely ineffective, but the Whistleblower Protection Enhancement Act passed in 2012 has sought to overcome some of these gaps. The recently passed Intelligence Authorization Act of 2014 prohibits retaliatory action against legitimate whistleblowers, and Presidential Directive 19 affirmed this mandate while presenting another method of authorized disclosure. The real powerhouse in the whistleblowing structure, however, is the office of Inspector General. Although Frank Snepp did not enjoy these recently introduced protections, he suffered consequences because he decided to disregard his contractual obligations he feared censorship. Thomas Drake also did not benefit from the most recent reforms when
he began leaking information. Although he claims to have used the legitimate methods of disclosure before “going nuclear,” he never made a robust attempt to file an IG report directly. Edward Snowden, who could have benefited from the WPEA and Presidential Directive reforms, decided instead to leak top-secret classified information to the press. In speaking about his experiences, Snowden is apt to quote Benjamin Franklin, stating, “He who sacrifice freedom for security deserves neither.” However, in the case of Snowden, this quotation rings hollow as could have raised his concerns about violations in the name of security through the authorized methods of disclosure. Instead, he never reportedly engaged his superiors, the appropriate IG, or Congress, and he must suffer the prescribed consequences for his actions.

Incentive, Shock, or Neither?
The Impact of Croatian Accession on Bosnia’s EU Negotiations

**Abstract**

What are the prospects for European Union accession in Bosnia, a country with a legacy of ethnic conflict and malfunctioning democracy? How might the accession of Croatia to the European Union affect this process? This paper analyses the current state of Bosnian politics through the lens of EU accession and considers the political and economic impact of Croatian accession.

A lack of incentive for Bosnian politicians to implement the governmental changes needed for Europeanization—the process of adopting European rules—has created a stagnant and intransigent political climate, one made more difficult by the Bosnian bureaucracy. Ethnic divisions hard-wired into the Bosnian political system by Article IV of the Dayton Agreement make the political costs of Europeanization and institutional reform much higher than those associated with the continuation of ethnicity-based parliamentary politics. However, Croatian accession (and the associated process of leaving the Central European Free Trade Agreement) will cause changes to the Bosnian economy, which heretofore has relied heavily on free trade with Croatia through CEFTA. A significant shock to the Bosnian economy caused by Croatian accession could trigger a political response, making Europeanization a viable alternative to the status quo. In order for the economic impact to be translated into politics, there must be an engaged populace willing to push for reform and translate their desire for Europeanization into a political force. Ultimately, I argue that the lack of effective inter-ethnic civil society and political mobilization in Bosnia will prevent significant political movement towards Europeanization, despite any economic discomforts caused by Croatia’s EU accession.

**Introduction**

Recent protests have made this a tumultuous time to study Bosnian politics. Starting in Tuzla in early February and spreading quickly to the rest of Bosnia, the protests—the largest Bosnia has ever seen—decry government corruption, poor economic conditions, and mangled privatizations. Politicians, rather than confront the substance of the protestors’ allegations, have been quick to use the demonstrations to promote their own goals.1

My research focuses on the origins of the stagnancy in Bosnian democracy and lack of progress towards EU accession. In this paper, I analyze the possible impact Croatian accession could have in pushing Bosnia towards the EU. I argue two points: first, that problems in Bosnia’s EU negotiations are due to a political structure that prioritizes staying in power and fosters corruption, and second, that Croatian accession will not change the status quo.

I draw on the external incentives model...