Barriers to Transparency: Constraints on the Efforts of Government Intelligence Whistleblowers

Barak Bullock | University of Texas, Austin

Edward Snowden’s disclosure of secret National Security Agency documents in 2013 was the most monumental leak of classified intelligence files in history. In the process of leaking the documents and sustaining their relevance in the public’s eyes, Snowden was faced with constraints on his ability to maximize the reformative power of the leak. These constraints were rhetorical and nonrhetorical, meaning they could be changed through discourse, or could not. Concepts from rhetorical scholarship, such as rhetorical situation and *topoi*, can help define these various constraints. The main analysis of this essay is an application of these concepts to editorials and news articles related to Snowden and other whistleblowers, such as Chelsea Manning, Julian Assange, Daniel Ellsberg, William Binney, and Thomas Drake. Snowden encountered the same constraints as these previous whistleblowers, suggesting they are persistent barriers that future whistleblowers will also have to confront.

On June 5th, 2013, British daily newspaper *The Guardian* published a classified top-secret intelligence document taken from the National Security Agency. It was a secret court order drafted by the Foreign Intelligence Surveillance Court, which revealed that the US telecommunications giant Verizon was being forced to hand over the metadata of millions of US customers to the NSA. With their metadata collection program, the NSA could identify callers’ numbers, locations, the time and duration of calls, and other unique identifiers of any American customer. The document proved that under the Obama administration, the phone records of millions of Americans were “being collected indiscriminately and in bulk—regardless of whether they [were] suspected of any wrongdoing” (Greenwald, “NSA”). This was only one of dozens of high-impact documents that were published in the following weeks and months.

Then, on June 9th, *The Guardian* posted an interview identifying the leaker of the document as Edward Snowden, an employee of NSA contractor Booz Allen Hamilton. Three weeks prior, Snowden secretly left his job, home, and long-time girlfriend in Hawaii for Hong Kong, where he leaked an enormous cache of classified documents to journalists Glenn Greenwald, Laura Poitras, and Ewen MacAskill. In the interview, Snowden stated the power to spy on others afforded to him as a senior analyst disturbed him, and declared that the public should decide whether they approve of the NSA’s activities (Greenwald, Poitras, and MacAskill). In an article posted June 11th, Snowden told *The Guardian*, “My sole motive is to inform the public as to that which is done in their name and that which is done against them” (Greenwald, Poitras and MacAskill). In little less than a week, the existence of the most powerful digital surveillance apparatus on Earth—and the story behind the man who exposed it—had been brought to light.
The Snowden leak—which officials asserted to contain approximately 1.8 million documents from American, British and Australian spy agencies—was called “the biggest theft of US secrets in history” by the Pentagon (Strohm and Wilber), and “the most catastrophic loss to British intelligence ever” by UK security expert Sir David Omand (“Snowden Leaks”). It unleashed a whirlwind of blockbuster headlines, commanded the attention of governments, news agencies, and citizens all around the world, and engendered dramatic debates on the ethics of whistleblowing, surveillance, and national security. Public discussion born from the leaks focused on the massive global surveillance program built by the US government, and on Snowden himself.

But Snowden was not the first to leak sensitive intelligence documents to the public in an act of political protest. There is a lineage of leakers that precedes Snowden in the realm of American government secrets. Among them is Chelsea Manning, who released thousands of military reports, State Department cables, and assessments of detainees from Guantanamo Bay to the publishing site WikiLeaks, and is currently serving a 35-year prison sentence (Tate); Julian Assange, the lead editor of WikiLeaks, who has been trapped in London’s Ecuadorean embassy since 2012 under the threat of extradition to the US for his involvement in Manning’s leak; Daniel Ellsberg, the leaker of the Pentagon Papers in 1971, who escaped a sentence of over 100 years when the government’s case against him was undone by the Watergate scandal. And lastly, Thomas Drake and William Binney, two NSA employees who were punished for speaking out against an intrusive and costly spying program named Trailblazer.

In the energetic discourse that surrounded their leaks, these five people were characterized in divergent ways. To their supporters, they were whistleblowers—“people who revealed wrongdoing within an organization to the public or to those in positions of authority” (“Whistleblower”)—and therefore were to be protected. To their opponents, the leakers’ efforts to unveil government secrets jeopardized precious lives or costly operations, and they deserved to be criminally prosecuted as traitors or terrorists. So are these people whistleblowers or not? This is an important question with far-reaching ramifications for how leakers like these are treated by the law.

Whistleblowers in all kinds of occupations are ostensibly protected from retaliation by their employers, since the act of whistleblowing is, at its core, an ethical decision to disclose illegal or unethical conduct by an agent or organization. These kinds of laws, such as the Whistleblower Protection Act of 1989, recognize the tremendous value that whistleblowers can offer in precipitating corrective measures, since problems no one knows of are not often solved. Ellsberg’s leak of the Pentagon Papers, which facilitated a massive erosion in support for the Vietnam War, is emblematic of the political impact that whistleblowing can have.

Legally speaking, defining someone like Snowden as a whistleblower or traitor has important consequences. Calling someone who leaks secrets a “whistleblower” explicitly praises their actions, and calls any retaliation against them into question. Those against the leaker’s actions may give him or her a condemnatory title like “traitor,” “spy,” or “terrorist,” which denounces their intentions as malicious, and their disclosures as dangerous. Even the seemingly-neutral “leaker” can be detrimental to a whistleblower’s case, since it does not connote legal protection. This makes the attribution of “whistleblower” an important
point of contention in discourse surrounding leak events, as it supports either the leaker’s legal protection or punishment.

But the consequences of these discussions extend beyond the fates of the leakers themselves. As mentioned earlier, the potential chance that foreign governments or terrorists will take advantage of leaked information, and that harm will come to innocents as a result, often accompanies the charges of betrayal. Conversely, if a government whistleblower reveals convincing evidence of wrongdoing without endangering lives, attempts to destroy the whistleblower diminish the reformatory power of those leaks, and may inhibit others from speaking out. It is clear, then, that the stakes involved in leaks of government intelligence are high—not just for leakers, but for the security of the nation as well—and warrant the public’s understanding of these issues.

One way to help the public reach this understanding is to analyze certain barriers that Snowden and the other leakers faced when attempting to bring attention to the waste, irresponsibility, or illegality they encountered. Many of these barriers are attacks on the leakers’ actions, while others are institutional or legal barriers. Surveying their experiences demonstrates that Snowden and the others each faced a combination of these constraints, which essentially served to deprive the leakers of whistleblower status. While Snowden’s disclosures are now available regardless of whether or not he is exonerated for releasing them, the rhetorical barriers he experienced and the ways that he and other whistleblowers are characterized conceivably deter other potential whistleblowers before they ever make headlines. Additionally, the impact of a leak can be minimized by its surrounding rhetoric, so the potential discoveries even in Snowden’s disclosures are still at stake. Because this pattern of rhetorical constraints effectively targets the ability of the leaker—and potential future leakers—to be defined as whistleblowers (along with the attendant protections of that term), it should not only be studied closely by the public, but should be examined within the purview of rhetoric.

Rhetorical scholarship gives us tools to analyze the effects of different definitions of terms and to identify a pattern of recurring arguments. If one is to observe how the definition of these leakers’ actions is manipulated by a recurring collection of constraints, then it is surely a job for rhetoric. Specifically, these constraints can be unpacked with two concepts from rhetorical theory, namely the rhetorical situation and topoi. I use these concepts in tandem to identify the struggles of these leakers as either rhetorical or nonrhetorical constraints, of which the rhetorical variations take the form of argumentative topoi. The rhetorical situation is defined below, and precedes an investigation of Snowden’s nonrhetorical constraints, while topoi will be introduced immediately before the section detailing Snowden’s rhetorical constraints.

My dichotomy of rhetorical and nonrhetorical constraints is derived from a now-standard concept in rhetorical scholarship, the rhetorical situation. The rhetorical situation, theorized by Lloyd Bitzer in 1968, consists of three main parts: an exigence, an audience and constraints. Bitzer wrote that an exigence is “an imperfection marked by urgency; a defect, an obstacle, something waiting to be done, a thing which is other than it should be” (6). Additionally, Bitzer says, “an exigence which cannot be modified is not rhetorical… An exigence is rhetorical when it is capable of positive modification and when positive modification requires discourse or can be assisted by discourse” (7). In other words,
problems we can solve with words are rhetorical exigencies, whereas things like hurricanes, or winter, are not.

Here, I apply Bitzer’s distinction between rhetorical and nonrhetorical exigences to constraints, which are defined as “circumstances which interfere with, or get in the way of, an advocate’s ability to respond to an exigence” (Jasinski 515). Essentially, this means there are constraints that can be overcome through discourse, and those that cannot. In the same way that a rhetorical exigence is a problem that can be solved with words, a rhetorical constraint describes an obstacle to addressing the exigence that can be dismantled with discourse. When imported into the context of intelligence leak events, the rhetorical constraints are the verbal and written attacks aimed at leakers, which can be refuted, while the nonrhetorical constraints consist of institutional and legal barriers to responsible disclosure, which are largely impervious to discourse. Bitzer’s rhetorical situation is comprised of three parts, but this analysis will be almost entirely devoted to discussing the constraints of Snowden’s rhetorical situation, rather than his exigence or his audience.

Studying these constraints primarily serves to demonstrate how Snowden and the other leakers were stripped of whistleblower protections, and raises important questions for the public to consider. For example, if a government intelligence worker attempts to blow the whistle on illegality using authorized channels of dissent—their superiors, their agency’s inspector general, the Department of Defense’s inspector general, and the Congressional intelligence committees in the House and Senate—and their efforts are unrewarded from within those channels, should bringing his or her knowledge to the public be considered treason, terrorism, or criminality?

Likewise, when leakers do disclose evidence of wrongdoing to the public and are ridiculed for putting American lives in danger, betraying the nation, or colluding with foreign governments and terrorists—statements which support the leakers’ punishment—should the public take these charges at face value? What if these charges are being levied by the same institutions whose crimes have been exposed, who have been tasked with preventing those crimes and who appear vested in preventing evidence of these crimes from surfacing?

Analyzing instances of these types of constraints on the efforts of American intelligence leakers can help the public answer these difficult questions, thereby improving their deliberation on the balance of national security and democratic civil liberty, especially on the treatment of leakers. But more specifically, looking at these constraints allows us to investigate whether whistleblowers are being treated unfairly by the government, or whether these leakers are deserving of the punishments they receive.

Therefore, my analysis consists of a historical investigation of the various constraints faced by Snowden and the other leakers already mentioned, beginning with their nonrhetorical constraints. This section focuses on the pursuit of accountability through official channels of dissent within the government, the viability of whistleblower protection laws, and the Obama administration’s frequent use of the Espionage Act to prosecute leakers. The second section focuses on the leakers’ rhetorical constraints: statements made against them in the aftermath of their public disclosures, including claims that the leakers are traitors, that they placed American lives at risk, and aided foreign governments and/or terrorists.
This analysis intends to demonstrate how leakers are deprived of whistleblower status, and to determine whether this is a benefit to the public.

**Nonrhetorical Constraints**

*Internal Channels of Dissent*

As mentioned earlier, Snowden’s three major nonrhetorical constraints were the government’s internal channels of dissent, whistleblower protection laws, and prosecution under the Espionage Act. Different whistleblowers before Snowden encountered some of these same obstacles to reform, but not all of them. Specifically, Binney and Drake’s experiences illustrate the failure of dissent channels, while Drake’s represent the failure of whistleblower protection laws. Lastly, Manning, Assange, Ellsberg, and Drake’s experiences all represent prosecution under the Espionage Act, but they are by no means the only whistleblowers who have been targeted in this way.

Snowden’s first nonrhetorical constraint was the efficacy of channels of dissent within the government. Ideally, legislation such as the Whistleblower Protection Act of 1989 would address issues of waste or abuse in the government by initiating internal investigations or disciplinary measures, but based on the experiences of Binney and Drake, these systems actually constitute a constraint (“Bill Text”). That is because for both Binney and Drake, using these internal channels did not result in any substantial reform, but did result in questioning by officials, raids on their homes, implication as an “unindicted co-conspirator” in Binney’s case, and actual charges filed under the Espionage Act in Drake’s case. Today, Binney and Drake are both free men who comment frequently on the Snowden case, but they still suffered retaliation for their exposure of government privacy violations.

According to journalist Jane Mayer, Binney worked for the NSA for 36 years and was considered “one of the best analysts in history.” Years before 9/11, Binney and others at the NSA created “ThinThread,” a program which would have analyzed massive amounts of email and phone data for potential threats, while leaving the data belonging to civilians without an outstanding arrest warrant encrypted. But Binney’s program was passed over for “Trailblazer,” a much less effective and more costly alternative, which did not protect civilian privacy. Trailblazer did not stop the 9/11 attacks from happening, and was abandoned in 2006 as “a $1.2 billion flop.” Binney retired from the NSA shortly after 9/11, when he realized that NSA management modified ThinThread to spy on American citizens in reaction to the attacks (Mayer).

Drake was a former senior executive at the NSA, who worked his first day on 9/11 (Mayer). He, like Binney, was of the minority who favored ThinThread over Trailblazer. Drake pursued the channels of dissent available in his position: he took his concerns to his boss, the third-highest-ranking member in the NSA, “to the agency’s inspector general, to the Defense Department’s inspector general and to the Congressional intelligence committees” (Shane). Their report to the Department of Defense is particularly illustrative of Binney and Drake’s nonrhetorical constraint on their abilities to use official channels of dissent.

Mayer writes that in September 2002, Binney and Drake issued a report to the Pentagon’s Inspector General’s office “extolling the virtues of the original ThinThread project and accusing the NSA of wasting money on Trailblazer.” Drake collected evidence for the report, while Binney—along with two other
retired analysts and a congressional staffer—filed it. The Inspector General’s follow-up report, which was completed in 2005 but not released to the public, was a “scathing document” which “hasten[ed] the end of Trailblazer.” However, the report did nothing to stop the other programs that would endure until Snowden’s time. Coincidentally, the DoD finished its report shortly before two New York Times reporters revealed the NSA was running a warrantless wiretapping program within the US. When federal officials went looking for the source of the Times leak, they found the Trailblazer critics instead (Mayer).

In the early morning of July 26th, 2007, “armed federal agents simultaneously raided the houses of Binney” and the other filers of the Inspector General complaint (Mayer). Earlier that year, Binney had been questioned by the FBI three times about any connection to the Times leak. Nevertheless, his home was raided, and computers, disks and documents were confiscated (Shane, Bronner and Savage). Months later, Drake was similarly raided, and the agents took “documents, computers, and books, and removed eight or ten boxes of office files from his basement” (Mayer). Though neither Binney nor Drake had anything to do with the Times leak, Drake had been communicating with a reporter from the Baltimore Sun about waste within the NSA, which mired him in an extended legal battle.

As Mayer writes, “under the law, such complaints are confidential, and employees who file them are supposed to be protected from retaliation.” However, officials claimed to have found classified documents among Drake’s possessions as a result of the raid, leading to several charges, including the willful retention of “national defense information” under the Espionage Act. Drake’s indictment threatened to put him in prison for 35 years (Mayer). Binney and the other signers of the Inspector General report were listed as “unindicted co-conspirators” in Drake’s case (Harris).

Eventually, Drake’s charges were dropped on the eve of his hearing in 2011. Because the judge ruled that the prosecution had obstructed the defense, Drake pleaded guilty to “a single misdemeanor count of exceeding his authorized use of an agency computer,” and was cleared of the ten or more charges accusing him of “illegally possessing classified information, obstructing the investigation into the leaks and lying to the FBI” (“Ex-Official”). Much like the first historical case of the Espionage Act being used against a leaker (Ellsberg), the case was thrown out, but the evidence of the nonrhetorical constraint faced by Binney and Drake is still intact. Their effort to use internal channels of dissent, though it sped up the demise of Trailblazer, was rewarded with intrusive raids, drawn-out prosecution, and potentially decades in prison.

It seems these channels of dissent operated poorly in the cases of Drake and Binney. The proper function of these channels depends on verbal and written deliberation between whistleblowers and authority figures, where convincing evidence of wrongdoing is exchanged for legal protection. Despite Trailblazer being eventually abandoned, the fact that Binney and Drake’s efforts to communicate within these dissent channels resulted in punishment rather than protection establishes these channels as a nonrhetorical constraint—a constraint that cannot be modified by discourse.

**Whistleblower Protection Laws**

Snowden’s second nonrhetorical constraint was his protection under whistleblower
protection laws. In this scenario, Drake was also an instructive example. Drake was ultimately a victim of the murky relationship between the Espionage Act and existing whistleblower protection laws. According to Bob Turner, a national security expert at the University of Virginia, the Espionage Act contains no explicit whistleblower protection, rendering those accused under it incapable of defending themselves in a courtroom (Greenberg). But Turner also noted that Snowden could have sought protection under the Intelligence Community Whistleblower Protection Act (ICWPA) of 1998 (Greenberg). As Jon Greenberg writes: “Under that law, Snowden could have raised his concerns with the Inspector General’s Office at the NSA or spoken to congressional intelligence committees… But others familiar with this legal landscape told us that no matter what, Snowden was still vulnerable.”

Snowden’s vulnerability stemmed from two sources. First, other whistleblowers from the intelligence community, such as Drake, had still been prosecuted under the Espionage Act, despite being protected under the ICWPA. As Spencer Kimball of Deutsche Welle wrote in January 2014:

“The ICWPA failed to adequately protect whistleblowers from retaliation. A former senior executive at the NSA, Drake blew the whistle on a failed surveillance program called Trailblazer. He used what the government calls “proper channels” to express his concerns about the program’s exorbitant cost and its lack of privacy protections, reaching out to his immediate supervisor, the office of the inspector general, and the congressional intelligence committees. When Drake felt he had exhausted internal channels of dissent, he contacted a reporter from the Baltimore Sun in 2005 to expose the illegality and waste of the Trailblazer program. As a result, “the federal government indicted him under the US Espionage Act for supposedly taking classified documents illegally, an allegation that unraveled before the trial. In the end, the government dropped the charges in exchange for Drake agreeing to plead guilty to one misdemeanor count of misusing a NSA computer” (Kimball).

Snowden’s second vulnerability was the lack of support for government contractors in the most recent whistleblower protection legislation. More legislation devoted to the protection of whistleblowers had indeed been ratified since the Drake case: In 2012, “Congress passed and President Obama signed the Whistleblower Protection Enhancement Act” and “Obama… issued [Presidential Policy Directive 19], extending whistleblower protections to the entire intelligence community” (Kimball). However, contractors such as Snowden had been omitted from the updated law (Davidson). Regardless, the precedent of Espionage Act prosecutions such as the Drake case seem to outweigh any whistleblower’s claim to protection under the law. William C. Banks, an expert on national security law at Syracuse University College of Law, told Deutsche Welle he believes criminal investigations into whistleblowers tend to override their protections: “I think the trump card is the criminal law. Regardless of whether the contractor or a regular employee of a US agency is blowing the whistle, if he or she is at the same time violating a criminal law of the United States, the whistleblower protection is worthless” (Kimball).

What the Drake case shows us is despite the ICWPA’s promise of protecting intelligence workers who report abuse or waste, practical experience demonstrates that whistleblowers still suffered retaliation, lending credibility to
the claims that the government’s channels for expressing dissent and legal protections of whistleblowers were ineffective. And if Banks is to be believed, the whistleblower protections that even certified government employees supposedly enjoy would be eclipsed by the Espionage Act, let alone contractors such as Snowden. That would go well beyond what it would take to demonstrate the nonrhetorical constraint on Snowden’s ability to address surveillance with legal protection. Therefore, it is the trail of Espionage Act prosecutions itself that constitutes the third major nonrhetorical constraint on Snowden’s position, which we can examine in light of the experiences of Manning, Assange, Ellsberg, and Drake.

**The Espionage Act**

In August 2013, two months after Snowden’s first leak, Manning was sentenced to 35 years in prison for his releases to WikiLeaks (Tate). Assange, WikiLeaks’ lead editor, fled to London’s Ecuadorean embassy in 2012, where he has lived ever since. Ellsberg faced over 100 years in prison in his trial, which, like Drake’s, was later dismissed. In each example, the Espionage Act is the common variable that explains the penalties each leaker faced.

The Espionage Act of 1917 is a World War I era law that “makes it an offence to take, retain or transfer knowledge ‘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’” (Borger). Though the bill was historically intended to punish spies, the Espionage Act has been increasingly deployed by the Obama administration to punish leakers. In fact, the Obama administration has indicted more defendants under the Espionage Act than all other administrations combined.

According to Greenberg, there have been eleven Espionage Act prosecutions since 1945, and seven of those have happened during Obama’s presidency.

As mentioned before, the most important thing about the Espionage Act as it pertains to Snowden is the omission of whistleblower protection. Ben Wizner, an ACLU lawyer and legal advisor to Snowden, said in 2014: “The laws under which Snowden is charged don’t distinguish between sharing information with the press in the public interest, and selling secrets to a foreign enemy” (McCarthy). In other words, claiming that he was a whistleblower who wanted to address abuse or waste was irrelevant. This paradox is at the heart of the Espionage Act cases brought against Snowden, Manning and Ellsberg, and it deprives whistleblowers—whether they are employees or contractors—of the protection that existing whistleblower laws supposedly offer.

Unsurprisingly, stripping whistleblowers of legal protection has several negative consequences for them. In the absence of prosecutorial misconduct, convictions under the Espionage Act may carry enormous prison sentences. But defendants charged under the Espionage Act have been imprisoned even before their trials. Before Manning’s hearing, she was “held for nine months in solitary confinement under conditions later deemed ‘excessive’ by a military judge” (McCarthy). On these pre-trial conditions, the UN’s special rapporteur on torture Juan E. Mendez said: “I conclude that the 11 months under conditions later deemed ‘excessive’ by a military judge” (McCarty). On these pre-trial conditions, the UN’s special rapporteur on torture Juan E. Mendez said: “I conclude that the 11 months under conditions later deemed ‘excessive’ by a military judge” (McCarty).
In Manning’s trial, the argument that Manning was a whistleblower attempting to reform injustice did not feature prominently in the defense’s case. It is unclear whether this was a deliberate strategy or a result of the judge’s discretion. The defense instead argued that “the government want[ed] to force [Manning] into… turning evidence against Assange,” and that Manning’s struggle with her gender identity impacted her decision-making (Radia; Zetter). It is difficult to believe the defense would forego arguing that Manning acted as a whistleblower without being barred from doing so, especially since the WikiLeaks files were later considered a catalyst for the democratizing Arab Spring movement of 2010–2011 (Walker). This hints at the Espionage Act’s chilling effect on the arguments available to legal defenders of whistleblowers.

Even leakers who avoid arrest and imprisonment, like Assange, can still find their freedom restricted. In December 2010, Australian diplomatic cables revealed “the Justice Department was conducting an ‘active and vigorous inquiry into whether Julian Assange can be charged under US law, most likely the 1917 Espionage Act’” (Dorling). Simultaneously, Assange was alleged to have sexually assaulted two women in Sweden in August 2010, and some called for his extradition to Sweden. Assange denied the allegations, and viewed extradition to Sweden as an attempt to put him in the hands of American authorities for prosecution in relation to WikiLeaks, prompting him to seek asylum at the Ecuadorean embassy (Addley). Assange has been confined to the Ecuadorean embassy in London since 2012, under the threat of immediate arrest if he walks outside its doors.

Daniel Ellsberg, the first case of a leaker being charged under the Espionage Act, faced a maximum penalty of 115 years when he was first indicted (“The Most Dangerous Man”). In the course of his trial, he was the first victim of the Espionage Act’s preclusion of a whistleblower defense argument in history. As a virtue of Ellsberg’s mistrial, Ellsberg himself can explain how he was barred from defending himself on the basis of addressing waste or abuse in the public interest:

“When I finally heard my lawyer ask the prearranged question in direct examination—Why did you copy the Pentagon Papers?—I was silenced before I could begin to answer. The government prosecutor objected—irrelevant—and the judge sustained. My lawyer, exasperated, said he ‘had never heard of a case where a defendant was not permitted to tell the jury why he did what he did.’ The judge responded: ‘well, you’re hearing one now’” (Ellsberg).

Similarly to Ellsberg, Drake’s defense was also prevented from including a discussion of whistleblowing. In response to the defense’s motion in favor of such a discussion, the prosecution argued that “Factually, the defendant’s theory of defense is nothing more than a justification defense wrapped in different sheep’s clothing… Evidence of the defendant’s whistleblowing efforts should be excluded because both the statute and Fourth Circuit law preclude a justification defense in this case” (“United States”).

These examples of the Espionage Act’s application demonstrate the heavy punishment facing leakers, as well as the deprivation of one of their most powerful defensive arguments: that they exposed secrets in order to address illegality, waste, or abuse encountered in their occupation. The Obama administration’s habit of Espionage Act prosecutions, along with the weakness of whistleblower protection laws and internal...
channels of dissent, represent potentially devastating constraints on a leaker’s ability to address the exigence of their rhetorical situation. As we know from Snowden’s story, he did not even attempt to pursue whistleblower protection like Drake and Binney did, and instead elected to leave the country entirely. It is evident, then, that the main avenues for those seeking whistleblower protection have been completely obstructed, and are insurmountable by discourse alone.

Rhetorical Constraints
Once Snowden evaded his nonrhetorical constraints, leaked the documents, and revealed his identity, he became the subject of verbal and written attacks. Like the nonrhetorical constraints before them, I argue these rhetorical constraints can be demonstrated by the experiences of leakers prior to Snowden. I collect these attacks into one major category I call the “damaged national security” topos. By defining this category as a topos, I intend to show that the lines of argument contained within it are recurrent over time and ready-made for leak situations, demonstrating their predictability.

Topoi, the plural of topos, is a Greek rhetorical term which has been broadly defined in different ways. The closest thing to a definition in the document of the term’s origin, Aristotle’s Rhetoric, is a general argumentative form or pattern that organizes individual iterations of a larger argument. However, this is not the only conception of topoi. According to Frans van Eemeren, over time topoi has become synonymous with “ready-made arguments.” “In contemporary literary scholarship the term topos has come to be used almost exclusively to refer to these ready-made arguments ‘or, by extension, to any theme or idea that has become a commonplace through repeated use.”’ Patricia Roberts-Miller similarly defines topos as “the recurrent ways that people tend to argue on a subject” (240). Due to the concept’s inherent ambiguity, she offers the term argumentative cliché as a possible replacement, but notes that this term potentially overlooks the reason for an argument’s frequent repetition (240). Two reasons why an argument might become cliché are that it is, in fact, a very sensible argument, or that “because it is repeated so often that people mistakenly think it has been proven” (240). Using topos rather than argumentative cliché allows us to consider these reasons why arguments are so often repeated while avoiding the word “cliché”’s embedded criticism.

Overall, the definition of topoi I use for this article takes traits of both definitions. That is, they are broad categories of arguments that have been made so common through repetition that they are often deployed immediately upon encountering familiar debates. Effort will also be spared to demonstrate the difference between this type of topos and topoi that are, in fact, legitimate arguments.

“Damaged National Security”
Many of the various attacks on Snowden can be contained within the “damaged national security” topos. This topos is a category of arguments which asserts that the national security of the US was damaged by the Snowden leaks. There are a variety of interdependent arguments contained within this topos. The first brands Snowden as a traitor and then invents negative consequences of the leaks, including that he put lives in danger by recklessly dumping the data, aided or worked for a foreign government, and/or helped terrorists in some way. In short:
• Snowden is a traitor.
• Snowden put lives in danger ("dumped the data").
• Snowden aided or is working for a foreign government.
• Snowden aided terrorists.

All of these sub-arguments carry the implicit messages that Snowden’s choice to leave the US and leak the documents makes his motivation for leaking the documents suspicious, that he cannot possibly be working for the public good, and therefore should not enjoy whistleblower protection. Examples of these arguments directed towards Snowden, as well as towards Manning, Assange, and Ellsberg, will be examined in this section.

Traitor
Soon after The Guardian published Snowden’s identity in early June 2013, Snowden was called a traitor, and the leaks an act of treason. Republican Speaker of the House John Boehner plainly stated, “He’s a traitor” (Johnson). New York Republican congressman Peter King said of Snowden: “This guy is a traitor. He’s a defector. He’s not a hero” (Kittle). That Sunday, former Vice President Dick Cheney told Fox News Snowden was a traitor, and suggested he could be a Chinese spy (Williams). Accusations of betrayal came from those on the left as well. California’s Democratic senator Diane Feinstein, who heads the Senatorial committee that oversees the NSA, said “I don’t look at this as being a whistleblower. I think it’s an act of treason” (Herb and Sink). Senate Majority Leader Harry Reid, a Democrat from Nevada, stated, “I think Snowden is a traitor, and I think he has hurt our country, and I hope someday he is brought to justice” (Hagar).

Whistleblowers before Snowden were called traitors too. Major Ashden Fein, the lead prosecutor in the case against Manning, said “[s]he was not a whistleblower; [s]he was a traitor” (Pilkington, “Bradley Manning a Traitor”). In popular right-wing media, Fox News’ Bill O’Reilly said “Manning is a traitor and should be given life and hard labor in a military prison.” Right-wing blogger Michael Van Der Galien called Assange a “ruthless traitor.” When Ellsberg leaked the Pentagon Papers in 1971, retired general and former chairman of the Joint Chiefs of Staff Lyman Lemnitzer said Ellsberg committed a “traitorous act,” and in Tom Wells’ biography of Ellsberg, Wild Man: The Life and Times of Daniel Ellsberg, Wells forwards the views of Ellsberg’s former associates at RAND that he was “a loathsome traitor” (Franklin; “Lemnitzer”).

Put Lives in Danger (“Dumped the Data”)
One of the central claims which often accompanied the charge of treason was that Snowden exposed information that would put American lives in danger. In his earlier statement, Boehner said the leak “puts Americans at risk” (Johnson). Current Director of National Intelligence James Clapper said the leaks compromised “measures used to keep Americans safe” (Gardner and Hosenball). Republican Congressman Mike Rogers, chairman of the House’s Intelligence Committee, articulated this point in the most literal sense by arguing Snowden should be charged with murder (Simons).

More importantly, critics asserted that the danger of the leaks came from the way Snowden leaked the documents, which was styled as a data “dump.” This nebulous term doesn’t have a formal definition, but essentially characterizes the leak of documents as so massive that responsibly scanning the leak for potentially damaging documents is impossible. This convenient argument, which relies simply on the size of the digital cache to support their contention that at
least something in the leak must be dangerous, has been used in multiple leak events. In the Snowden story, this point was made earliest by Jeffery Toobin of *The New Yorker*, who, crucially, compared Snowden’s leak to Manning’s leak: “It’s not easy to draw the line between those kinds of healthy encounters and the wholesale, reckless dumping of classified information by the likes of Snowden or Bradley Manning. Indeed, Snowden was so irresponsible in what he gave the Guardian and the Post that even these institutions thought some of it should not be disseminated to the public.” Over six months later, Zachary Keck of *The Diplomat* cited the way Snowden “dumped” the documents as the reason why he should never be called a whistleblower: “Had Snowden been a whistleblower interested in protecting the American constitution, he would have carefully collected information documenting NSA overreach in spying on Americans… Instead, he collected an apparently unknowable amount of information (unknowable to both him and the NSA) and dumped it on the doorsteps of largely foreign newspapers.”

This argument was used relentlessly against Assange and Manning, who, together, published thousands of military reports and State Department cables to WikiLeaks in 2010. Harold Koh, a legal advisor for the State Department, said WikiLeaks “could place at risk the lives of countless innocent individuals—from journalists to human rights activists and bloggers to soldiers to individuals providing information to further peace and security” (Youssef). Then Secretary of State Hillary Clinton said Assange and Manning’s leak “puts people’s lives in danger, threatens our national security and undermines our efforts to work with other countries to solve shared problems” (“Clinton Condemns”). Admiral Mike Mullen, chairman of the Joint Chiefs of Staff, targeted Assange specifically: “Mr. Assange can say whatever he likes about the greater good he thinks he and his source are doing… But the truth is they might already have on their hands the blood of some young soldier or that of an Afghan family” (Jaffe and Partlow).

Support for the claim that Manning and Assange put lives in danger was also based on Manning’s method of leaking the documents, and was also portrayed as a data “dump.” During Manning’s trial, Captain Joe Morrow told judge Denise Lind that Manning “systematically harvested hundreds of thousands of documents from classified databases and then dumped that information on to the internet into the hands of the enemy” (Usborne). Thomas Ricks, writing for *Foreign Policy*, said “I opposed what Manning did. I thought his actions were reckless. He did a data dump, making secret information public without knowing what it was or what he was really doing.” Toobin and Keck’s characterization of the Snowden leak closely resembles these arguments used against Manning, which rely on painting the method of disclosure as thoughtless, unexamined, and dangerous.

**Aiding or Working for a Foreign Government**

The accusation that Snowden was a foreign agent or was at least indirectly helping foreign governments was also a prominent attack. At different points in the leak timeline, Snowden was styled to have been a Chinese spy (based on his escape to Hong Kong) and a Russian spy (based on his asylum bid in Moscow), and in both instances, the charges of spying and merely helping ran parallel to one another. Toobin sparked the discussion on the possibility of Chinese involvement in the leaks soon after Snowden’s identity was revealed:
The overriding fact is that Hong Kong is part of China, which is, as Snowden knows, a stalwart adversary of the United States in intelligence matters. Snowden is now at the mercy of the Chinese leaders who run Hong Kong. As a result, all of Snowden’s secrets may wind up in the hands of the Chinese government—which has no commitment at all to free speech or the right to political dissent. And that makes Snowden a hero?

As mentioned earlier, Cheney suggested Snowden’s choice of Hong Kong was evidence that he was a Chinese spy:

“I’m suspicious because he went to China. That’s not a place where you would ordinarily want to go if you are interested in freedom, liberty and so forth,’ Cheney said, adding: ‘It raises questions whether or not he had that kind of connection before he did this.’ Cheney suggested that Snowden could still be in possession of confidential data and that the Chinese would ‘probably be willing to provide immunity for him or sanctuary for him in exchange for what he presumably knows or doesn’t know.” (Williams)

Though Toobin and Cheney do not match on whether Snowden is a spy, they both associate Snowden’s motives with the status of press freedoms in mainland China. However, Cheney extends this by not simply warning that the documents are within reach of Chinese authorities, but that Snowden has long-planned to compromise US secrets to China in exchange for protection.

Later that month, Jane Perlez and Keith Bradsher of the New York Times supplied ammunition for the argument that Snowden was aiding a foreign government indirectly. In their report of China’s decision to let Snowden leave Hong Kong, they wrote, “Two Western intelligence experts, who worked for major government spy agencies, said they believed that the Chinese government had managed to drain the contents of the four laptops that Mr. Snowden said he brought to Hong Kong, and that he said were with him during his stay at a Hong Kong hotel.” Though this assertion that the Chinese government drained four laptops full of NSA documents was disputed for its over-reliance on anonymous government sources, it was repeated by multiple commentators, including The New Yorker, “D.C. gossip sheets, right-wing outlets, and diaries at Democratic Party sites,” but most notably by Clinton (Greenwald, “Snowden”). Speaking on domestic spying programs at the University of Connecticut in April 2014, Clinton said: “It struck me as—I just have to be honest with you—as sort of odd that he would flee to China, because Hong Kong is controlled by China, and that he would then go to Russia—two countries with which we have very difficult cyber-relationships, to put it mildly” (Roller).

Here, in a vague suggestion similar to Cheney’s, Clinton insinuates Snowden’s choices of refuge may either increase the likelihood that Snowden is working for a foreign government, or that of a foreign government has come to possess the NSA documents, compromising US cyberpower in some way. Clinton continued, “I think turning over a lot of that material—intentionally or unintentionally—drained, gave all kinds of information, not only to big countries, but to networks and terrorist groups and the like. So I have a hard time thinking that somebody who is a champion of privacy and liberty has taken refuge in Russia, under Putin’s authority” (Roller).

Here, Clinton develops Toobin’s point about aiding foreign governments. We see her
mention the possibility of “intentionally or unintentionally” helping, and her reference to the “drained” information, which is used to support the claim that Snowden provided information to “terrorist groups and the like.” Lastly, she disputes Snowden’s motives on grounds he is “under Putin’s authority,” insinuating Snowden works for Russia.

After Snowden’s arrival in Russia on June 23rd, Philip Ewing, writing for Politico, captured Toobin’s point that Snowden was placing the documents within dangerous proximity of a foreign power, except this time it was Russian authorities. Ewing wrote, two days after Snowden’s arrival, “The fact remains that Snowden’s flight from Hong Kong on Sunday has put him right into the lair of Russia’s infamous intelligence service. And whether or not he started out intending to talk with foreign intelligence officers, that may be what has happened.”

Prominent congressional conservatives doubled down on the theory that Snowden was a Russian agent. In 2013, Rogers stated unequivocally that Snowden was colluding with Russian spies: “Many don’t find it odd he is in the loving arms of an SVR [Russia’s External Intelligence Service] agent right now in Moscow. I do” (Simons). Months later, Senator John McCain said there was “not a doubt in his mind” that Snowden was working for Russia (Spiering).

Though there doesn’t seem to be a consensus among all of Snowden’s critics as to whether he was a spy or simply convenient for foreign powers, Keck summarized what they would likely all agree on: that Snowden provided the countries where he traveled with information: “Snowden seeking refuge in first China and then Russia nearly guarantees that the governments in these countries have gained a treasure trove of valuable information on NSA operations against their countries.” In Keck’s view, no matter which variation of the attack is true, spy or not spy, the result is the same: Snowden damaged national security by delivering sensitive classified documents into our rivals’ hands.

Like Snowden, Ellsberg was described as a spy on multiple occasions, although for the Soviet Union. Trevor Timm, writing for the Freedom of the Press Foundation, explains: “shortly after he leaked the top secret Vietnam War study, the Nixon administration made a concerted effort to paint him as a Soviet spy in the press, using anonymous quotes and non-existent ‘secret’ evidence.” Those efforts are found in three New York Times articles from 1973 and 1974. The first article covered testimony given to the Senate Watergate committee by John D. Ehrlichman, a former White House aide for the Nixon administration, who suggested “that Dr. Ellsberg delivered copies of the Pentagon papers to the Soviet embassy” (Timm). As Ellsberg’s attorney Leonard B. Boudin later summarized, Ehrlichman claimed “the Pentagon papers had been given in 1971 to the Soviet Embassy and implied that this might have been done by... Dr. Daniel Ellsberg, or with his knowledge” (Timm). The second article from 1973 covered the alleged reasoning behind the Nixon administration’s decision to form the Plumbers unit. Essentially, the Nixon administration feared Ellsberg had given the Soviets US secrets, and therefore compromised an American spy by bringing on the Senate Watergate committee hearings, so they formed the Plumbers to discredit Ellsberg and distract from the hearings (Timm). In 1974, the Times reported on an internal government memo, which directly likened Ellsberg to former US “spies,” on the basis
that he claimed to disregard federal law to answer a higher calling: “Most of what Daniel Ellsberg has said in public since he acknowledged stealing the Pentagon Papers seems calculated to position him as having responded to an order of morality higher than his onetime solemn undertakings to his country. This rationale, let it be remembered, was earlier employed by atomic spies Klaus Fuchs, David Greenglass, Morton Sobell and Bruno Pontecorvo” (Timm).

As the Ellsberg case demonstrates, the accusations of espionage were thrown at both him and Snowden. In both cases, the charges of espionage were often made in the absence of convincing evidence, and accompanied campaigns of discrediting the whistleblower.

Aided or Working for Terrorists
The same can be said of the argument that the leak helped terrorists understand or circumvent US counterterrorism efforts. Boehner, describing the NSA’s surveillance programs, said “these were important national security programs to help keep Americans safe and give us tools to fight the terrorist threat that we face” and that the disclosures “show our adversaries what our capabilities are” (Johnson). Senator Bill Nelson, writing for Daily News, wrote “the Department of Justice should bring charges against [Snowden] for deliberately taking classified information... in such a way that our enemies can use it against us.” As we’ve already seen, Clinton also stated that the leaks helped terrorists, when she said: “I think turning over a lot of that material... gave all kinds of information... to networks and terrorist groups” (Roller). Shawn Turner, a spokesperson for Clapper, perhaps articulated the most complete version of the argument that the leaks would help terrorists: “We’ve been clear that these leaks have been unnecessarily and extremely damaging to the United States and the intelligence community’s national security efforts... As a result of these disclosures, terrorists and their support networks now have a better understanding of our collection methods and, make no mistake about it, they are taking counter measures” (Dilanian and Serrano).

In this variation of the “damaged national security” topos, Manning and Assange were also Snowden’s predecessors. After WikiLeaks published American intelligence files supplied by Manning, both Manning and Assange came under fire from accusations of helping terrorists or being terrorists themselves. Malcolm Rifkind, chairman of the Parliamentary Intelligence and Security Committee in Britain, said the leaks were “a gift to any terrorist (group) trying to work out what are the ways in which it can damage the United States” (Lister). Moving beyond the claim of aiding terrorists, both Vice President Joe Biden and Republican Senator Mitch McConnell called Assange a “high-tech terrorist” (Curry; MacAskill). In a similar vein, King urged that WikiLeaks be designated a “foreign terrorist organization,” saying it “posed a clear and present danger to the national security of the United States” (Kennedy).

Manning was exposed to this same line of argument in his pre-trial hearing in 2013. Fein said Manning “knowingly gave intelligence through WikiLeaks to the enemy,” which he asserted was Al Qaeda in the Arabian Peninsula and “all other enemies with Internet access” (Gosztola). Interestingly, the prosecution avoided the hurdle of proving Manning had knowledge that the files would end up in the hands of Al Qaeda, instead “arguing that Manning is guilty of the aiding the enemy charge because he knew that al Qaeda has access to the Internet, and to
WikiLeaks in particular” (Sledge, “Bradley”). These arguments culminated in Manning’s charge of aiding the enemy, which was eventually dropped, but nonetheless constituted the most serious charge against Manning, and formed the base of the prosecution’s arguments that Manning aided Al Qaeda or other groups.

**Broken, or Just Fine?**

In the past two sections, *rhetorical* and *non-rhetorical* constraints of Snowden’s rhetorical situation have been defined. The experiences of Manning, Assange, Ellsberg, Binney, and Drake showed the government’s internal channels of dissent, whistleblower protection laws, and Espionage Act prosecutions compromised leakers’ efforts to expose information, and that these barriers were impenetrable by discourse; they were *non-rhetorical* constraints. From Snowden, Manning, Assange, and Ellsberg, we know that leakers were routinely attacked with variations of the “damaged national security” *topos*, but this constraint could be combated with their own discourse.

We now face the primary question raised by this investigation: are these constraints evidence of a system which is unjustly depriving whistleblowers of their entitled legal protection, or of a system that is rightly punishing violators of US national security?

To this day, no evidence supporting any of the contentions within the “damaged national security” *topos* with regard to Snowden has come to light. No evidence showing Snowden’s leak put any American military or civilians in danger has surfaced, nor that he worked with a foreign government (Sledge, “One Year After”; “No Evidence”). Binney himself argued in an interview with *USA Today* that terrorists gained no advantage from Snowden’s leak (Eisler and Page). And the argument that Snowden is a traitor for taking his information abroad seems tenuous given his inability to take advantage of whistleblower protection at home. This is what makes the “damaged national security” *topos* a product of baseless repetition rather than a legitimate critique. It seems, then, that many leakers deserving of legal protection for their insights into government abuse have been unfairly denied this right.

Ideally, an informed population would be capable of appropriately weighing a dissenting voice against an institutional condemnation, and would know whether to demand the punishment of a dangerous criminal, or a redress of grievances from an unscrupulous government. With the help of rhetorical tools like the *rhetorical situation* and *topoi*, the public can anticipate and reject the predictable routine of attacks levied against whistleblowers in future leak events, and view their leaks as a response to our broken whistleblower protection system. As a country which values civil liberty and the rule of law, we should view the constraints analyzed in this article as pernicious barriers to justice for whistleblowers and transparency from our government.
Acknowledgements
I would like to thank my thesis advisor Patricia Roberts-Miller for her fantastic guidance on this project and for encouraging me to submit my writing to Young Scholars In Writing. I would also like to thank Professors Annette Vee and Doug Downs for their excellent help throughout the revision process at YSW, which made my entry what is today.

Works Cited


