Cleveland State Law Review

Volume 63 | Issue 1 Note

2014

Top Secret—The Defense of National Security Whistleblowers: Introducing a Multi-Factor Balancing Test

Patrick M. Rahill

TOP SECRET—THE DEFENSE OF NATIONAL SECURITY WHISTLEBLOWERS: INTRODUCING A MULTI-FACTOR BALANCING TEST

PATRICK M. RAHILL*

* J.D. Candidate, 2015. Thank you to my family and friends for their support throughout this process. Special thanks to the current and past members of the Cleveland State Law Review for their helpful insights, edits, and support. I'd like to dedicate this article to my parents, Katie and Pat Rahill, for their continued love, encouragement, and guidance throughout my life.

I. INTRODUCTION

In the summer of 2013, the United States was hit with what some have called one of the most significant national security leaks in U.S. political history.[1] Beginning in May 2013, Edward Snowden began leaking documents that detailed a massive surveillance program orchestrated by the National Security Agency ("NSA").[2] Snowden then fled the country, and eventually ended up in Russia, where he has been granted temporary asylum.[3]

Back in the United States, the exposure of the NSA surveillance program has led to significant public debate including concerns about civil rights,[4] demands for reform,[5] and proposed legislation.[6] The United States government has also weighed

---

[1] Glenn Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (June 9, 2013), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

[2] *Id.*; *see also* Glenn Greenwald & Ewen MacAskill, *Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data*, THE GUARDIAN (June 11, 2013), http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining.

[3] Isabel Gorst & Joby Warrick, *Snowden Leaves Moscow Airport to Live in Russia*, WASH. POST (Aug. 1, 2013), http://www.washingtonpost.com/world/europe/snowden-leaves-moscow-airport-to-live-in-russia/2013/08/01/2f2d1aba-faa9-11e2-a369-d1954abcb7e3_story.html. Snowden's asylum ended on July 31, 2014 at midnight. *Snowden's Asylum Status in Russia Ends*, USA TODAY (Aug. 1, 2014), http://www.usatoday.com/story/ news/world/2014/08/01/russia-snowden-asylum/13454055/. He has reapplied for asylum in Russia, and will remain there until a decision is made. *Id.*

[4] Glenn Greenwald, *Major Opinion Shifts, in the US and Congress, on NSA Surveillance and Privacy*, THE GUARDIAN (July 29, 2013), http://www.theguardian.com/commentisfree/2013/jul/29/poll-nsa-surveillance-privacy-pew. A Pew poll found for the first time in a decade, the majority of Americans are more concerned about the government infringing on their civil liberties than about a potential terrorist attack. *Id.*

[5] Craig Timberg, *Tech Companies Urge Lawmakers to Reform NSA Programs*, WASH. POST (Oct. 31, 2013), http://www.washingtonpost.com/business/technology/tech-companies-urge-lawmakers-to-reform-nsa-programs/2013/10/31/f100ced6-4264-11e3-a751-f032898f2dbc_

in on the incident, charging Snowden with three felonies, including two under the infamous Espionage Act of 1917[7] ("Espionage Act").[8]

This marks the eleventh time the United States has prosecuted a national security leaker under the Espionage Act.[9] Prior to the Obama administration there had been three–Daniel Ellsberg, Samuel Morison, and Lawrence Franklin.[10] Since Obama took office, there have been seven prosecutions, with Snowden marking the eighth.[11] A common theme has developed among these eight Obama prosecutions: lower-level leaker employees are being prosecuted more frequently than higher-ranking officials.[12] As scholars have noted, "[t]his imbalance is particularly troubling when the government is trying to silence the very leaks that the press and the public find most valuable: those that disclose what the government wants to keep secret for political reasons."[13] In contrast, upper-level official leaks are usually made with the approval of the administration.[14] While potentially valuable, these leaks are usually one-sided in order to "shape public discourse on a given issue."[15] "Leaks by lower-level government employees," however, "are typically made without approval and often reveal serious wrongdoing in the government."[16]

This imbalance poses a significant problem for our nation: transparency is essential to a healthy democracy. In order to hold public officials accountable, an informed electorate is necessary, and an electorate that is continuously fed

---

story.html. Facebook, Google, Apple and three other leading technology companies have called for substantial reforms to the U.S. government's surveillance programs. *Id.*

[6] There are now several major pieces of legislation going through Congress that would introduce at least some reform of the NSA. Ewen MacAskill & Gabriel Dance, *NSA Files: Decoded*, THE GUARDIAN (Nov. 1, 2013), http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded. The more far-reaching proposal would be the Intelligence Oversight and Reform Act, which would ban the collection of internet communication data, close loopholes that allow for snooping on Americans without a warrant, reform the FISA courts, and provide some protection for companies faced with handing over data to the NSA. *See id.*

[7] Espionage Act of 1917 (Espionage Act), 18 U.S.C.A. § 792 (West 2014).

[8] Politico, *Document: Edward Snowden Unsealed Complaint*, (June 21, 2013), *available at* http://www.politico.com/story/2013/06/edward-snowden-complaint-unsealed-93181.html.

[9] Aubrey Bloomfield, *8 Whistleblowers Charged with Violating the Espionage Act Under Obama*, POLICY.MIC (June 23, 2013), http://www.policymic.com/articles/50459/8-whistleblowers-charged-with-violating-the-espionage-act-under-obama.

[10] *Id.*

[11] *Id.*

[12] David McCraw & Stephan Gikow, *The End to an Unspoken Bargain? National Security and Leaks in a Post-Pentagon Papers World*, 48 HARV. C.R.-C.L. L. REV. 473, 494-95 (2013).

[13] *Id.*

[14] *Id.*

[15] *Id.* at 495.

[16] *Id.* McCraw and Gikow provide an example to highlight this point. "leaks about government-sponsored torture and the government's widespread eavesdropping program did not appear to be sanctioned by high-level government officials." *Id.*

"favorable" information by the administration is an uninformed one. Historically, government whistleblowers of "classified information have played an important role in informing the public throughout our country's history."[17] Today's prosecutions, however, have effectively deterred these important players in our nation's history.[18] Most national security whistleblowers are afraid to enter the gray zone where prosecution may result.[19] This reluctance not only perpetuates government abuse in this area, but also keeps the constituency ignorant of important public official action.

In order to ensure that this valuable source of information remains a viable option, federal law should employ a multi-factor test to determine whether or not a defendant-leaker should be acquitted of the charges. Part II of this paper offers background on the current state of affairs by looking at the applicable law and how courts have interpreted that law. Part II also offers a more detailed look into the events that transpired in the summer of 2013 involving Snowden and the NSA. Part III introduces the reader to the proposed multi-factor test that provides a concrete analytical framework to evaluate each leak. Part A suggests that the leaker's intent play a more significant role in the analysis. Part B details how a court would analyze the threat to national security the leak would cause. Part C of the analysis suggests that an evaluation of the recipient of the leaked information should play a determining influence on the conviction. Part D weighs the public debate sparked from the leak. After detailing each of the proposed factors, each will be applied to Snowden's case as an example of how a court would employ the multi-factor test. Finally, Part IV offers a brief conclusion.

II. NATIONAL SECURITY WHISTLEBLOWERS AND THE CURRENT LAW TODAY

A. Conflicting Values: Transparency v. National Security

As mentioned briefly above, one of the keys to democracy and an informed public is a transparent government. In a self-governing society, citizens must know what their representatives are doing if they are to govern themselves intelligently. As Senator Ron Wyden correctly pointed out:

> It is a fundamental principle of American democracy that laws should not be public only when it is convenient for government officials to make them public. They should be public all the time, open to review by adversarial courts, and subject to change by an accountable legislature guided by an informed public. If Americans are not able to learn how

---

[17] Mary-Rose Papandrea, *Lapdogs, Watchdogs, and Scapegoats: The Press and National Security Information*, 83 IND. L.J. 233, 254 (2008). For example, leaks of secret or classified information have led to the public discovery of several questionable practices, including the treatment of prisoners in Abu Ghraib and Guantanamo Bay. *Id.* at 255.

[18] Leonard Downie Jr., *The Obama Administration and the Press: Leak Investigations and Surveillance in Post-9/11 America*, CPJ: COMMITTEE TO PROTECT JOURNALISTS, 2 (Oct. 10, 2013), http://cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php.

[19] *Id.*

> their government is interpreting and executing the law then we have effectively eliminated the most important bulwark of democracy.[20]

At the same time, a completely open government may compromise our national security.[21] Keeping certain information confidential, especially when it relates to national security, is necessary to keep our nation safe from the various threats of war. In the wake of September 11, 2001, our nation has entered a new war, a "war on terror."[22] Unlike before, where the United States could achieve a relative peace through "conventional policies of deterrence and punishment,"[23] the current enemy is "not a nation state against which the U.S. can retaliate."[24] This new enemy is one willing "to commit suicide for their cause," and has the "potential to wreak large-scale havoc and destruction" in a variety of ways.[25] As our nation has seen, "there appears to be no effective way to protect the nation by deterring or punishing the enemy."[26] Accordingly, in our objective to protect our nation, prevention of terrorist activities becomes all-important.[27] Attempting to achieve the proper balance between these two conflicting ideals–transparency on one hand, security on the other—has proved difficult.

In 1966, Congress tried to balance these two ideals by passing the Freedom of Information Act ("FOIA").[28] The purpose behind the law was to give the public the right to access information concerning the federal government.[29] The information that is accessible, however, is limited by the FOIA itself. The law specifically exempts those materials properly classified pursuant to Executive Orders.[30] Furthermore, it excludes from disclosure "documents that are 'specifically exempted from disclosure by statute.'"[31] Thus, the FOIA incorporates the "sweeping secrecy provisions of such statutes as the Central Intelligence Act and the National Security Act."[32] Beyond the fact that FOIA litigation takes a tremendous amount of time, money, and patience, concerned citizens must have an idea what they are looking

---

[20] Senator Ron Wyden, Remarks as Prepared for Delivery for the Center for American Progress Event on NSA Surveillance (July 23, 2013), *available at* http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-104.pdf.

[21] Geoffrey R. Stone, *On Secrecy and Transparency: Thoughts for Congress and a New Administration*, AMERICAN CONSTITUTION SOCIETY FOR LAW AND POLICY, 3 (2008).

[22] George W. Bush, President, U.S., Address to a Joint Session of Congress (Sept. 20, 2001) (transcript *available at* http://edition.cnn.com/2001/US/09/20/gen.bush.transcript/).

[23] Stone, *supra* note 21, at 1.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] Freedom of Information Act (FOIA), 5 U.S.C.A. § 552 (West 2014).

[29] McCraw & Gikow, *supra* note 12, at 476.

[30] 5 U.S.C.A. § 552(b)(1)(A)-(B) (West 2014).

[31] McCraw & Gikow, *supra* note 12, at 476.

[32] *Id.* at 476-77 (citations omitted).

for.[33] This is often impractical unless a leak has already provided information about the activity.[34] Thus, when viewed as a whole, the current state of affairs seems to favor secrecy in the name of national security over transparency.[35]

Executive orders provide the means through which presidents influence policy decisions. Since 1940, successive presidents have utilized executive orders relating to the classification of documents.[36] The current executive order relating to classification is Executive Order No. 13,526.[37] This Order sets out the prerequisites that outline how to classify documents,[38] as well as the appropriate classification level.[39] In order to classify information, four conditions must be met.[40] First, an original classification authority ("OCA") must classify the information.[41] An OCA may be the president,[42] vice president,[43] agency heads,[44] officials designated by the president,[45] or United States government officials delegated the authority pursuant to this Executive Order.[46] Second, the information at hand must be owned by, produced by or for, or under the control of the United States government.[47] Third, the information must fall within one or more of the categories of information listed in

---

[33] Mary-Rose Papandrea, *Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment*, 94 B.U. L. Rev. 449, 471 (2014).

[34] *Id.*

[35] When FOIA is viewed in context with various statutory provisions that punish leaks of national security information, such as the Espionage Act discussed more fully below, it becomes clear that FOIA is an inadequate vehicle for asserting the right to obtain such information. *See id.* at 477.

[36] Patricia L. Bellia, *WikiLeaks and the Institutional Framework for National Security Disclosures*, 121 YALE L.J. 1448, 1511 (2012).

[37] EXEC. ORDER NO. 13, 526, 75.2 C.F.R. 707 (2010).

[38] *See id.* at § 1.1(a)(1)-(4).

[39] *See id.* at § 1.2(a). "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe. *Id*. at (a)(1). "Secret" shall be applied to information, the unauthorized disclosure of which reasonable could be expected to cause serious damage to the national security that the OCA is able to identify or describe. *Id.* at (a)(2). "Confidential" shall be applied to information, the authorized disclosure of which reasonably could be expected to cause damage to the national security that the OCA is able to identify or describe. *Id.* at (a)(3).

[40] *Id.* at § 1.1(a).

[41] *Id.* at § 1.1(a)(1).

[42] *Id.* at § 1.3(a)(1).

[43] *Id.*

[44] *Id.* at § 1.3(a)(2).

[45] *Id.*

[46] *Id.* at § 1.3(a)(3); *see also id.* at § 1.3(c) (detailing the delegation of authority process).

[47] *Id*. at § 1.1 (a)(2).

Section 1.4 of the Executive Order.[48] Fourth and finally, the OCA must determine that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the OCA is able to identify or describe the damage.[49]

While classifying documents pursuant to this procedure seems sound in theory, in practice it has led to disturbing results. As one can tell from reading Executive Order No. 13,526, many government officials may be classified as an OCA. Furthermore, the determining guidelines are subjective,[50] leaving the potential for massive amounts of "classified" documents. This result has occurred, as many scholars have noted that the quantity of classified materials is prohibitively massive today.[51] Some have estimated that anywhere between "50% and 90% of documents are misclassified."[52] Furthermore, without scrutinizing those classifying documents, there exists a huge risk that classified information may be false,[53] or that the government exaggerates the harm that the information may present.[54] Additionally, "the current classification scheme does not prohibit the classification of information revealing illegal government behavior."[55] This again adds to the abundance of classified information. Overclassification presents a problem[56] for the courts to consider when analyzing national security leaks, and Part III.B offers a suggestion on how to address that problem.

---

[48] *Id.* at § 1.1(a)(3); *see also id.* at § 1.4(a)-(h) (outlining the classification categories). For example, information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to national security, and it pertains to one or more of the following categories: intelligence activities (including covert action), intelligence sources or methods, or cryptology being one of them. *Id.* at § 1.4(c).

[49] *Id.* at § 1.1(a)(4).

[50] *See also* Papandrea, *supra* note 33, at 475 (arguing that classification is more of an art rather than a science, often based on subjective rather than objective considerations).

[51] Robert Bejesky, *National Security Information Flow: From Source to Reporter's Privilege*, 24 ST. THOMAS L. REV. 399, 403 (2012).

[52] McCraw & Gikow, *supra* note 12, at 485.

[53] Bejesky, *supra* note 51, at 408.

[54] Richard Moberly, *Whistleblowers and the Obama Presidency: The National Security Dilemma*, 16 EMP. RTS. & EMP. POL'Y J. 51, 120 (2012).

[55] Papandrea, *supra* note 33, at 477. Professor Geoffrey Stone would typecast this use of classification as an "illegitimate government secret." *See infra* Part III.B.1 for further explanation.

[56] Bellia, *supra* note 36, at 1520 (stating that overclassification is a significant contributing factor for why national security leaks keep occurring).

B. Statutory Punishment and Protections Afforded National Security Whistleblowers

1. The Espionage Act and the Statutory Regime Criminalizing Leaks

By disclosing national security information, national security whistleblowers may face charges under the Atomic Energy Act,[57] Intelligence Identities Protection Act,[58] and the Federal Larceny Statute.[59] Yet, the main source of punishment, although controversial, still remains the Espionage Act.[60] The Espionage Act was passed in 1917 in order to punish acts of interference with the foreign relations, and the foreign commerce of the United States, to punish espionage, and to better enforce the criminal laws of the United States.[61] Over the years, it has been applied to national security whistleblowers.[62]

Three main sections of the Espionage Act are applicable in national security whistleblower cases—Sections 793, 794 and 798. Section 793 restricts the gathering, retention, and dissemination of national security defense information.[63] It punishes those individuals who disseminate or retain material "willfully."[64] Furthermore, it punishes those who have reason to believe that information pertaining to national defense could injure the United States or benefit a foreign nation,[65] friend or foe.[66] Finally, the way the statute is written, the information disclosed does not have to be

---

[57] Atomic Energy Act, 42 U.S.C.A. § 2011 (West 2014). This Act protects the secrecy of information relating to nuclear energy and weapons. Papandrea, *supra* note 17, at 270. As applied to whistleblowers, "[it] subjects to criminal penalties anyone who 'communicates, transmits, or discloses' documents or information 'involving or incorporating restricted data' with the 'intent to injure the United States' or advantage a foreign nation, or who has 'reason to believe such data' would have that effect." *Id.* at 272.

[58] Intelligence Identities Protection Act, 50 U.S.C.A. § 3121 (West 2014). This Act prohibits the identification of covert agents. Papandrea, *supra* note 17, at 274. As applied to government whistleblowers, the Act prohibits anyone from disclosing classified information that identifies a covert agent to any individual not entitled to receive it. *Id.* at 274-75.

[59] 18 U.S.C.A. § 641 (West 2014). It imposes criminal penalties not only on anyone who "embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof," but also anyone who" receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted." Papandrea, *supra* note 17, at 277. For an article arguing that all leakers should be prosecuted under this statute, see Jessica Lutkenhaus, *Prosecuting Leakers the Easy Way: 18 U.S.C. § 641*, 114 COLUM. L. REV. 1167 (2014). The government charged Snowden under this provision as well. *See* Politico, *supra* note 8.

[60] 18 U.S.C.A. § 792 (West 2014).

[61] *Id.*

[62] *See e.g.*, United States v. Gorin, 312 U.S. 19, 20-21 (1941).

[63] 18 U.S.C.A. § 793 (West 2013).

[64] *Id.*

[65] *Id*.

[66] Papandrea, *supra* note 17, at 265.

damaging,[67] meaning that it does not have to harm any United States' interest. Most leakers are commonly charged under § 793(d) of the Espionage Act.[68]

Section 794 pertains to the classic case of espionage. It concerns the transfer of national defense information, and prohibits its disclosure to an agent of a foreign government.[69] Additionally, it requires a showing that the whistleblower has the "intent or reason to believe that [the information] is to be used to the injury of the United States or to the advantage of a foreign nation.[70] A person found guilty under this section may also face the death penalty.[71] Section 794(b) is applicable only "in time[s] of war"[72] and punishes those who intend to communicate the information "to the enemy."[73]

Section 798's scope for punishment "is staggering."[74] It bans dissemination of classified information concerning the communications intelligence activities of the United States.[75] It requires that the whistleblower do this "knowingly" and "willfully."[76] Furthermore, it does not require a showing that the information would pose any harm to the United States or provide an advantage to a foreign power.[77] Lastly, the section takes no consideration as to whether or not the information was properly classified.[78]

As noted, the Espionage Act has been utilized to punish individuals since 1917, and it has been relatively unmodified since then. This has led many to call for amending the Act to fit today's high-tech world.[79] Furthermore, many fear the potentially broad application of the Act to punish institutions like the press.[80] Lastly, while concerns over the constitutionality of the Act have unsuccessfully been

---

[67] *Id.*

[68] Papandrea, *supra* note 33, at 509.

[69] 18 U.S.C.A § 794 (West 2014).

[70] *Id.* at § 794(a).

[71] *Id.*

[72] *Id.* at § 794(b). This perhaps may have broader implications however, considering how often the United States is involved in foreign conflict.

[73] *Id.*

[74] Papandrea, *supra* note 17, at 269.

[75] 18 U.S.C.A. § 798 (West 2013).

[76] *Id.* at § 798(a).

[77] *Id.* at § 798; *see also* Papandrea, *supra* note 17, at 270.

[78] Papandrea, *supra* note 17, at 270.

[79] *See, e.g.*, Jamie L. Hester, *The Espionage Act and Today's "High-Tech Terrorist*," 12 N.C. J.L. & TECH. ON. 177 (2011) (advocating revision of the Act in the advent of computer technology and the internet).

[80] *See, e.g.*, Robert D. Epstein, *Balancing National Security and Free-Speech Rights: Why Congress Should Revise the Espionage Act*, 15 COMMLAW CONSPECTUS 483 (2007) (calling for Congress to revise the Espionage Act in order to more effectively carry out the Act's purpose of guarding and protecting the national defense of the United States, while at the same time protecting the fundamental First Amendment rights of American citizens).

challenged in the courts,[81] many call for a rewriting of the Act to better delineate exactly what it punishes.[82]

2. The Intelligence Community Whistleblower Protection Act and Other Statutory Protections

While there exist statutes that protect national security whistleblowers, those protections are few. The general federal whistleblower law, known as the Whistle Blower Protection Act of 1989,[83] explicitly excludes employees of the Federal Bureau of Investigation, the Central Intelligence Agency, the NSA, and other national security agencies.[84]

Congress sought to remedy this in 1998 by passing the Intelligence Community Whistleblower Protection Act ("ICWPA").[85] The Act protects those whistleblowers who disclose matters of "urgent concern"[86] through the required steps. The Act requires that the disclosure first be made to the appropriate Inspector General ("IG") or a designee.[87] That IG then assesses the credibility and decides whether or not to pursue its merits.[88] If the IG determines the report to be credible, he or she must forward the report to the head of the intelligence agency within fourteen days.[89] A flaw remains, however, in the fact that "IGs are appointed and removable by the President, and they cannot even report serious wrongdoing to Congress without first giving the relevant agency head the opportunity to delete sensitive information."[90]

The ICWPA additionally provides that the employee-whistleblower may report directly to congressional intelligence committees only if certain conditions are met.[91] First, he or she may only do so if "the Inspector General fails to accurately transmit the report within the 14 day calendar period"[92]. Second, "the employee, before making such a contact, [must] furnish[] the head of the activity, through the Inspector General, a statement of the employee's complaint and notice of the employee's intent to contact the intelligence committees directly."[93] Finally, "the

---

[81] *See, e.g.*, United States v. Morison, 604 F. Supp. 655, 658-59 (D. Md. 1985).

[82] *See* Epstein, *supra* note 80.

[83] Whistle Blower Protection Act, 5 U.S.C.A. § 2302 (West 2014).

[84] *Id.* at § 2302(a)(2)(C)(ii).

[85] Papandrea, *supra* note 17, at 247.

[86] *Id.* An urgent concern is a serious or flagrant violation of law or executive order, a false statement to Congress (or withholding information), or the reprisal against a person who reported a matter. *Id.*

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] Papandrea, *supra* note 33, at 473. Papandrea highlights this flaw by mentioning that the CIA's IG "has never exposed major wrongdoing within the agency that would have otherwise gone unexposed." *Id.*

[91] *Id.* at 493.

[92] Papandrea, *supra* note 17, at 247.

[93] *Id.* at 247-48.

employee [must] obtain[] and follow from the head of the activity, through the Inspector General, direction on how to contact the intelligence committees in accordance with appropriate security practices."[94]

The ICWPA gives the appearance of protecting national security whistleblowers, but in reality it does not provide any substantive protection from retaliation.[95] For example, those employees who bypass the above procedures and report directly to Congress are not protected from retaliation.[96] Retaliation may occur through revocation of security clearance, "a decision that is generally not subject to independent judicial review."[97] Retaliation may also result in an employee's "indefinite suspension or termination."[98] This lack of protection "reduces an employee's willingness to disclose wrongdoings and therefore gives the President almost unchecked authority to keep national security information secret."[99] The Congressional Research Service supported this conclusion in 2005, finding that "one reason federal employees leak information to the press is that the government has failed to provide adequate protection for whistleblowers."[100]

Thomas Drake's experience provides an insight into the lack of protection offered by the ICWPA. A former senior executive at the NSA, Drake had concerns about "massive waste, mismanagement, illegality, and a willingness to compromise the privacy of U.S. citizens."[101] Drake reported these concerns through the requisite channels within the Intelligence Community: his immediate supervisors, the NSA's inspector general, the Department of Defense's Inspector General, and congressional intelligence committees.[102] When nothing resulted from these efforts, Drake went to a *Baltimore Sun* reporter with the information that was not even classified.[103] Despite those mitigating facts, the government charged Drake under the Espionage Act.[104] As Drake himself noted, "[b]y following protocol, you get flagged–just for raising

---

[94] *Id.*

[95] Moberly, *supra* note 54, at 109.

[96] Papandrea, *supra* note 17, at 247.

[97] *Id.* at 248; *see also* Cheney v. Dep't of Justice, 479 F.3d 1343, 1352 (Fed. Cir. 2007) (holding that neither the Board nor the courts could review the underlying merits of an agency's decision to suspend a security clearance).

[98] Papandrea, *supra* note 17, at 248.

[99] Moberly, *supra* note 54, at 109.

[100] Papandrea, *supra* note 17, at 248; *see also* LOUIS FISHER, CONG. RESEARCH SERV., RL33215, NATIONAL SECURITY WHISTLEBLOWERS 12-16 (2005).

[101] Jesselyn Radack & Kathleen McClellan, *The Criminalization of Whistleblowing*, 2 AM. U. LAB. & EMP. L. F. 57, 63 (2011).

[102] *Id.*

[103] *Id.*

[104] *Id.* at 64. The government eventually dropped all ten felony charges, and Drake pleaded guilty to a single misdemeanor charge of "exceeding his authorized use of a computer," with a recommendation from the government of no jail time and no fine. *Id.* at 65.

issues. You're identified as someone they [the government] don't like, someone not to be trusted."[105]

Drake's case is not the only example showing the lack of protection offered by the ICWPA. Both William (Bill) Binney and J. Kirk Wiebe experienced similar NSA retaliation measures due to their activities. Both worked for the NSA, where they served for decades.[106] Similar to Drake, they blew the whistle on mismanagement surrounding a program known as "Trailblazer."[107] Together, they voiced their concerns about the program though the appropriate channels, sharing the information with the Department of Defense Inspector General and Congress.[108] Despite following the requisite steps, no one at NSA was held accountable for what some have called "one of the worst intelligence failures in history."[109] In response, then-NSA General Michael Hayden issued an internal memo accusing whistleblowers of betraying the agency, stating that "[a]ctions contrary to our decisions will have serious adverse effect on our efforts to transform NSA and I cannot tolerate them."[110] As a result of their whistleblowing, "Binney was demoted to a different position, so that he would not have easy access to the Congressional oversight committees" and Wiebe, a recipient of the Meritorious Civilian Service Award, the NSA's second highest distinction, was left off potential career advancement projects.[111] Witnessing continuous wasteful, fraudulent, and unconstitutional behaviors on behalf of the NSA, both men retired shortly thereafter.[112]

Stories like those above exemplify that current statutory protection for national security whistleblowers is illusory, if not non-existent. Knowing that the requisite ICWPA procedures usually lead nowhere, whistleblowers must turn to different areas for protection. As Part 3 will demonstrate below, courts provide little protection for national security whistleblowers as well.

3. National Security Whistleblowers and the Courts

As demonstrated above, there is very little statutory protection offered to a national security whistleblower under the ICPWA. Accordingly, those individuals

---

[105] Thomas Drake, *Snowden Saw What I Saw: Surveillance Criminally Subverting the Constitution*, THE GUARDIAN (June 12, 2013, 7:00 AM), http://www.theguardian.com/commentisfree/2013/jun/12/snowden-surveillance-subverting-constitution.

[106] *NSA Whistleblowers William (Bill) Binney and J. Kirk Wiebe*, GOV'T ACCOUNTABILITY PROJECT, http://www.whistleblower.org/bio-william-binney-and-j-kirk-wiebe (last visited Aug. 29, 2014).

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *Id.* Despite being retired from the NSA, both men continued to face retaliation from the NSA. *Id.* The NSA prevented their newly formed private company from getting work, and caused the contracts they did procure to end abruptly. *Id.* Furthermore, when the *New York Times* ran their warrantless wiretapping story, both Binney and Wiebe were targeted as being the source behind the leak. *Id.* Agents ransacked their homes despite not being involved in the story whatsoever. *Id.*

must rely on the courts' interpretation of the applicable statutes to their individual cases. In *United States v. Gorin*, the Supreme Court dealt with the interpretation of the predecessor provision of Section 793 of the Espionage Act.[113] The Court required that those prosecuted must have acted in bad faith.[114] Furthermore, it found that "confidentiality" is a question of fact for the courts to determine, as negligence upon disputed facts is determined.[115]

The most important case for national security whistleblowers is *United States v. Morison*.[116] Samuel Morison was charged with releasing three classified photographs to a British magazine where he had been working.[117] The court in *Morison* held that the Espionage Act passed constitutional scrutiny[118] and that it applied to national security whistleblowers.[119] As to intent, the court held that under sections 793(d) and (e), the only scienter required is the wilful transmission or delivery to one not entitled to receive it.[120] Furthermore, it was no defense that delivery of documents to a person not entitled to receive them was done with "good intentions."[121] Accordingly, *Morison* abolishes the "bad faith" requirement, and endorses a wilful *mens rea*.

Finally, the case *United States v. Rosen*[122] involved two lobbyists who received and unlawfully communicated classified information.[123] The two lobbyists were charged under Section 793(e) of the Espionage Act for the unauthorized possession of and wilful communication of information to any persons not entitled to receive it.[124] The two defendants then moved to dismiss, which the court ultimately rejected.[125] In rejecting the motion to dismiss, however, Judge Ellis interpreted Section 793 to require that the prosecution prove beyond a reasonable doubt that the defendants knew that the United States held the information at issue closely, that the disclosure of such information could potentially harm the United States, and that the defendants knew that the individuals to whom they communicated the information

---

[113] Gorin v. United States, 312 U.S. 19, 19 (1941).

[114] *Id*. at 20-21.

[115] *Id.* at 32; *see also* James A. Goldston et al., *A Nation Less Secure: Diminished Public Access to Information*, 21 HARV. C.R.-C.L. L. REV. 409, 432-33 (1986).

[116] United States v. Morison, 604 F. Supp. 655, 657 (D. Md. 1985).

[117] *Id.* at 657.

[118] Statute was not unconstitutionally vague by failing to give fair warning what documents are covered. *Id.* at 659. Furthermore, the statute is not overbroad where a limiting instruction is given. *Id.* at 660-61.

[119] Statute applies to the "leaking" of information to the press. *Id.* at 660.

[120] *Id.* at 658-59.

[121] *Id.* at 663.

[122] United States v. Rosen, 445 F. Supp. 2d 602, 607-08 (E.D. Va. 2006).

[123] *Id.*

[124] *Id.* at 610, 615.

[125] *Id.* at 610, 645.

lacked authority to receive it.[126] Additionally, Judge Ellis found that Section 793 requires a bad faith element for conviction.[127]

C. Snowden's Summer of 2013

In early June and July of 2013, *The Guardian* and *The Washington Post* began disclosing documents that detailed three expansive NSA surveillance programs.[128] The first program requires telecommunication companies, like Verizon, to provide to the NSA on a daily basis "all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."[129] The second program, known as "PRISM," allows the NSA to access "audio and video chats, photographs, e-mails, documents, and connection logs" collected by nine U.S. internet giants like Google and Facebook.[130] The third program, known as XKeyscore, "provides analysts with the capacity to mine content and metadata generated by e-mail, chat, and browsing activities through a global network of servers and internet access points."[131]

A few days later, Edward Snowden revealed himself as the leaker of the above documents.[132] Snowden was a former technical assistant for the CIA, as well as an employee of the defense contractor Booz Allen Hamilton.[133] For four years prior to the summer of 2013, he worked at the NSA as an employee of various outside contractors.[134] It was as an employee for the CIA working in Geneva, Switzerland where Snowden began thinking about exposing government secrets.[135] In Geneva, Snowden became "disillusioned…about how [his] government functions and what its impact is in the world."[136] He realized that he "was part of something that was doing more harm than good."[137]

---

[126] *Id.* at 625; *see also* Epstein, *supra* note 80, at 503-04.

[127] *Rosen*, 445 F. Supp. 2d at 626.

[128] David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 63 (2013); *see also* Kennedy Elliot & Terri Rupar, *Six Months of Revelations on NSA*, WASH. POST (Dec. 23, 2013), http://www.washingtonpost.com/wp-srv/special/national/nsa-timeline/.

[129] Gray & Citron, *supra* note 128, at 63-64. While this program does not allow for the collection of content, like conversations, telephony metadata includes a caller's identity, location, and social network. *Id.* at 64.

[130] *Id.*

[131] *Id.*

[132] Greenwald, *supra* note 1.

[133] *Id.*

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] *Id.*

Snowden's biggest fear post-leak was that the public would not embrace these disclosures, and that no public debate would be facilitated.[138] It is safe to say, as many commentators have pointed out, this fear has not come to fruition. As mentioned above, the exposure of the NSA surveillance programs has led to significant public debate including concerns about civil rights, demands for reform, and proposed legislation.[139] The international community has also become outraged, as reports indicate that the U.S. Government may have been spying on international allies, including Germany.[140] These allegations have forced the Obama Administration to weigh in, too. On January 17, 2014, President Obama "made a forceful call to narrow the government's access to millions of Americans' phone records as part of an overhaul of surveillance activities."[141]

III. FUTURE WHISTLEBLOWER PROTECTION: INTRODUCTION TO THE MULTI-FACTOR TEST

As demonstrated above, the time is ripe for the court to allow a national security whistleblower to provide a defense for his or her actions. As will be explained in further detail below, four main factors should be scrutinized when this defense is offered: (1) the whistleblower's intent; (2) the threat to national security; (3) the recipient of the classified documents; and (4) the public debate sparked by the leak.

A. First Factor—The Requirement of Bad Faith on Behalf of the Whistleblower

1. A "Bad Faith" Element

In order to punish a national security whistleblower, a "bad faith" element of intent must be required. The government must still prove the required intent to each of the elements,[142] but an additional element of "bad faith" must be shown. Specifically, a showing of bad faith would require that (1) the whistleblower knew that the publication of information would create a clear and imminent danger of

---

[138] Glenn Greenwald, *Edward Snowden's Worst Fear Has Not Been Realised – Thankfully*, THE GUARDIAN (June 14, 2013, 2:00 PM), http://www.theguardian.com/commentisfree/2013/jun/14/edward-snowden-worst-fear-not-realised.

[139] *See* Greenwald, *supra* note 4; Timberg, *supra* note 5; MacAskill & Dance, *supra* note 6.

[140] *See* Laura Smith-Spark, *Germany's Angela Merkel: Relations with U.S. 'Severely Shaken' Over Spying Claims*, CNN (Oct. 24, 2013, 1:10 PM), http://www.cnn.com/2013/10/24/world/europe/europe-summit-nsa-surveillance/ (detailing the soured relations with Germany, as well as with Mexico and Brazil).

[141] Ellen Nakashima & Greg Miller, *Obama Calls for Significant Changes in Collection of Phone Records of U.S. Citizens*, WASH. POST (Jan. 17, 2014), http://www.washingtonpost.com/politics/in-speech-obama-to-call-for-restructuring-of-nsas-surveillance-program/2014/01/17/e9d5a8ba-7f6e-11e3-95c6-0a7aa80874bc_story.html; *see Say What: Breaking Down Obama's NSA Speech,* WASH. POST, http://www.washingtonpost.com/wp-apps/say-what/say-what-breaking-down-obamas-address-on-nsa-reforms/ (last visited Aug. 29, 2014), for a video and copy of the speech. (second citation might be cited as state of the union address instead, what do you think?)

[142] That is, that he (1) knew the information related to national defense, (2) knew that injury to the national defense was likely or knew the information would advantage an enemy of the United States, (3) intentionally communicated information, and (4) knew that the person was not entitled to receive it. United States v. Rosen, 445 F. Supp. 2d 602, 611 (E.D. Va. 2006).

grave harm to national security;[143] and (2) that the whistleblower knew or was reckless in not knowing that the publication of this information was "non-newsworthy."[144]

Additionally, implicit in the intent analysis is consideration of the whistleblower's motive. If the whistleblower discloses information for selfish reasons such as monetary enrichment, fame, recognition, or career advancement, he or she must be punished. Conversely, if the whistleblower acted unselfishly with the intention to inform the public, that evidence must weigh in favor of acquittal. As this article emphasizes, no two leaks are created equal.[145] A court cannot assume that all releases of national security information will be benign in motivation or result.[146] A bad faith requirement tolerates those whistleblowers who leak for courageous and patriotic reasons and punishes those who leak maliciously, due to a variety of factors.[147]

As noted above, the requirement of "bad faith" is not a novel concept.[148] The Court in *Gorin* required that those prosecuted must have acted in bad faith.[149] Furthermore, as Judge Ellis's opinion stated in *Rosen*, Section 793 requires a bad faith element for conviction when applied to those who receive confidential information from a source.[150] Federal whistleblower protection law must embrace this holding in *Gorin* and Judge Ellis's opinion in *Rosen*, and allow for acquittal of those national security whistleblowers who leak government documents in the absence of bad faith.

It can be expected that this element may be difficult to determine in practice. Accordingly, it is predictable that any national security whistleblower would simply state that he or she acted in good faith when disseminating the information. Problematic as this may seem, there are ways around it. "Bad faith" would be a determination of fact, left for the fact-finder to determine. The fact-finder would be able to assess the credibility of evidence, witnesses, surrounding circumstances, and the whistleblower, should he or she choose to testify. Modern jurors make these determinations every day in criminal cases nationwide. Thus, it is logical that this practice applies to national security whistleblower cases as well.

---

[143] Geoffrey R. Stone, *Prosecuting the Press for Publishing Classified Information*, 2 FIU L. REV. 93, 95 (2007).

[144] *Id.*; *see also* discussion of "non-newsworthy" information *infra* Part III.B.

[145] McCraw & Gikow, *supra* note 12, at 498.

[146] Bellia, *supra* note 36, at 1505.

[147] *Id.*

[148] In fact, there is great support that the original framers of the Espionage Act thought it necessary that bad faith element be necessary for conviction. *See* Goldston, *supra* note 115, at 421-25. Supporters of the 1917 bill stressed that "the objective was to punish spying in the classic sense, and not to restrict public discussion of defense matters." *Id.* at 422. Supporters of the 1950 amendments again stressed their exclusive application to classic espionage. *Id*. at 423. Most significantly, "the final House report on the amendments explained that, under the espionage statutes, 'unauthorized revelation . . . can be penalized only if it can be proved that the person making the revelation did so with an intent to injure the United States." *Id.*

[149] Gorin v. United States, 312 U.S. 19, 20-21 (1941).

[150] United States v. Rosen, 445 F. Supp. 2d 602, 607-08 (E.D. Va. 2006).

Furthermore, while intent is given great weight in this analysis, it should not be determinative. Each national security leak is different than the next, and convictions must be determined on a case-by-case basis. For example, suppose a national security whistleblower acts in bad faith when disclosing the information, but the information disclosed is highly beneficial to public debate. Again, the jury must determine the question of whether the benefits of the disclosure outweigh the bad intent of the whistleblower. If the information disclosed is highly beneficial, it seems likely that the whistleblower should face less severe sanctions. Conversely, imagine a scenario where a national security whistleblower acts in good faith when disclosing the information, but the information, unbeknownst to the whistleblower, is highly damaging to national security.[151] Situations like this place the nation in grave danger, and that fact must outweigh a whistleblower's good intent.

In short, the national security whistleblower's bad faith in disclosure is an important factor that must be considered by the courts. That said, it should not be determinative. Each of the following factors must be weighed against the bad faith factor in order to determine, if necessary, the appropriate level of punishment.

2. Daniel Ellsberg and the "Pentagon Papers:" Exemplar of Good Faith

One way a fact-finder may reach a determination concerning the national security whistleblower's intent is to look at how much information he or she disclosed. Take, for example, the source behind the "Pentagon Papers," Daniel Ellsberg. In 1971, *The New York Times* began publishing a massive 1967-1969 government study concerning U.S. involvement in Southeast Asia.[152] The news publishers, *The New York Times* and *The Washington Post*, possessed forty-three volumes of the Defense Department's history of the Vietnam War,[153] several cables, position papers, and memoranda exchanged among high-level administrative officials.[154]

While it seems like the news publishers had a magnitude of information, they did not have everything. Ellsberg specifically chose not to disseminate "four volumes dealing with diplomatic relations."[155] Ellsberg withheld these documents "out of concern that their release would disrupt diplomatic efforts to end the war."[156] Ellsberg's goal was not to place the nation in grave danger, but rather to inform the public of U.S. involvement in a highly controversial war.[157] Even though the

---

[151] Some scholars refer to this scenario as the "mosaic theory." *See* Christina E. Wells, *State Secrets and Executive Accountability*, 26 CONST. COMMENT. 625, 635 (2010). According to the mosaic theory, "intelligence work is 'akin to the construction of a mosaic' where an item of information seems (or is) insignificant standing alone, but actually has great importance to one who pieces the innocuous information together." *Id.*

[152] Bellia, *supra* note 36, at 1454-55.

[153] McCraw & Gikow, *supra* note 12, at 483.

[154] Bellia, *supra* note 36, at 1455.

[155] McCraw & Gikow, *supra* note 12, at 483.

[156] Bellia, *supra* note 36, at 1466.

[157] *See 1971 Year in Review: The Pentagon Papers*, UPI (1971), http://www.upi.com/Archives/Audio/Events-of-1971/The-Pentagon-Papers/?spt=nil&d=n. As Daniel Ellsberg said himself, "I felt that as an American citizen, as a responsible citizen, I could no longer cooperate in concealing this information from the American public." *Id.*

government argued the potential harm of publication of these materials, no harm resulted.

3. Samuel Morison and His Quest for Employment

A national security whistleblower's bad faith can likewise be inferred from the surrounding circumstances. Most cases involve the whistleblower acting in a selfish manner, and not in the public's interest. The case of Samuel Morison provides an illustrative example. Morison worked at the Naval Intelligence Support Center, with top-secret clearance.[158] He also worked part-time for the British publisher of *Jane's Fighting Ship* and *Jane's Defence Weekly*.[159] He was convicted for disseminating pictures and summaries of naval secrets.[160] The court found that Morison "was making available secret material to . . . *Jane's* as a means of furthering his application for employment by *Jane's* and for payment."[161] Although there was no direct statement about compensation, past practice indicated that "when [Morison] had in the past furnished material of interest, *Jane's* had paid [Morison]."[162]

Morison's case exemplifies this bad faith standard in two regards. First, it is clear that he acted in pursuit of his own interests. He disseminated classified information to a potential employer for hope of employment and monetary gain. Second, his leaks, although claiming to be patriotic, were not made in the public interest. The leaks involved a detailed report about an explosion at the shipyard, and pictures of that explosion. Neither would be of any interest to the public, yet Morison decided to disclose such information in bad faith.

4. Edward Snowden: Daniel Ellsberg of the Twenty-First Century?

Difficulties arise when applying this factor to Snowden's case today. Everything we know of Snowden's intent comes from sources that believe he is either a "hero" or a "traitor." Publications will thus be slanted in accordance with that view. Nonetheless, these sources provide early glimpses into what evidence may be introduced should Snowden face trial.

An interesting place to start is Edward Snowden's "Manifesto" that he published a few months after the initial disclosures.[163] Although brief, it allows an outsider to ascertain Snowden's state of mind. The NSA programs in his mind were "not only a threat to privacy," but also "threaten[ed] freedom of speech and open societies."[164]

---

[158] William E. Lee, *Deep Background: Journalists, Sources, and the Perils of Leaking*, 57 AM. U. L. REV. 1453, 1479 (2008).

[159] *Id.*

[160] United States v. Morison, 844 F.2d 1057, 1060 (4th Cir. 1988). Specifically, he was sentenced to two years in prison for violating (1) section 793(d) of the Espionage Act that proscribes the willful disclosure of national defense information to "any person not entitled to receive it," (2) section 793(e) that prohibits the unauthorized possession and retention of classified information, and (3) a statute that punishes the theft of government property. *See* Lee, *supra* note 158, at 1480.

[161] *Morison*, 844 F.2d at 1062.

[162] *Id.* at 1061.

[163] Edward Snowden, *Snowden: A Manifesto for the Truth*, DER SPIEGAL (Nov. 5, 2013), http://www.globalresearch.ca/a-manifesto-for-the-truth/5356919.

[164] *Id.*

When encountered with programs such as these, Snowden believes that "[w]e have a moral duty to ensure that our laws and values limit monitoring programs and protect human rights."[165] Understanding and controlling these problems can only be accomplished "through an open, respectful and informed debate."[166] When the government is dishonest and hides matters of public importance, Snowden believes it is up to citizens to "fight suppression" of this type of information, and to tell the truth.[167] Snowden's own text comes across as a plea for transparency and an informed and courageous citizenry. His "Manifesto" implies that his intent behind these disclosures was to inform the public, both nationally and worldwide, about the presumed powers that governments possess.

Interviews with Snowden after the incident confirm this. Despite coming forward, Snowden repeatedly says that he does not want media attention.[168] He insists rather, he wants the focus of the debate "to be about what the U.S. government is doing."[169] Snowden stated that his "sole motive is to inform the public as to that which is done in their name and that which is done against them."[170] Despite having a very comfortable life prior to the disclosures, he was willing to sacrifice much of his own freedom in order to secure "privacy, internet freedom and basic liberties for people around the world."[171] Snowden claims that he was not motivated by fame or money, but rather he felt that "[t]he government has granted itself power it is not entitled to" with these programs.[172] While Snowden admires Chelsea Manning,[173] he believes there is one important distinction between him (he) and Manning:

> I carefully evaluated every single document I disclosed to ensure that each was legitimately in the public interest. There are all sorts of documents that would have made a big impact that I didn't turn over, because harming people isn't my goal. Transparency is.[174]

Snowden obviously then sees himself more akin to Daniel Ellsberg, describe above, as selectively releasing documents that he believed would not result in harming the nation.

---

[165] *Id.*

[166] *Id.*

[167] *Id.*

[168] Greenwald, *supra* note 1.

[169] *Id.* According to Snowden, he "really want[ed] the focus to be on these documents and the debate which [he] hop[ed] [would] trigger among citizens around the globe about what kind of world we want to live in." *Id.*

[170] *Id.*

[171] *Id.*

[172] *Id.*

[173] Formerly known as Bradley Manning, the source of the largest leak of government documents in U.S. history, leaking over 700,000 diplomatic cables and military reports on the Iraq and Afghan wars to WikiLeaks. *See* Bloomfield, *supra* note 9.

[174] Greenwald, *supra* note 1.

Yet others do not buy into Snowden's "for the public" mantra. Some suggest that Snowden has been planning on releasing these documents since 2011, when he was working for Dell.[175] The argument continues by insinuating that Snowden purposefully switched employers to Booz Allen Hamilton in order to "gain access to additional top-secret documents that could be leaked."[176] Others suggest that Snowden disclosed these documents with fame and recognition in mind, rather than the public interest.[177] Jeffrey Toobin suggests that Snowden is "a grandiose narcissist" who unveiled "legally authorized programs" because they "failed to meet his own standards of propriety."[178] Snowden, Toobin believes, set a bad precedent for government employees and contractors to "sabotage programs they don't like."[179] *Fox News* analyst Ralph Peters argues that Snowden's leaks constituted "treason," and that the death penalty should be his punishment.[180] Peters believes that Snowden's action constituted "foreign policy making," something he is not capable of doing.[181]

As stated above, it is difficult to ascribe a motive to Snowden based purely on these sorts of publications. However, these sources exemplify how a fact-finder must judge the motives of Snowden—based on a totality of the circumstances. A jury makes findings as to motive frequently; they are more than competent to do so in Snowden's case.

B. Second Factor–Type of Document Leaked

In most cases, national security whistleblowers get into trouble when they leak classified documents. Most of the time, the classification level determines the perceived threat to national security. For example, as mentioned above, the current Order[182] classifying documents has three levels, each corresponding to a different threat to national security.[183] As a nation at war more often than at peace,[184] some

---

[175] Mark Hosenball, *Snowden Downloaded NSA Secrets While Working for Dell, Sources Say*, REUTERS (Aug. 15, 2013), http://www.reuters.com/article/2013/08/15/us-usa-security-snowden-dell-idUSBRE97E17P20130815.

[176] *Id.*

[177] Roger Simon, *The Slacker Who Came in from the Cold*, POLITICO (June 11, 2013, 5:17 AM), http://www.politico.com/story/2013/06/the-slacker-who-came-in-from-the-cold-92534.html.

[178] Jeffrey Toobin, *Edward Snowden is No Hero*, THE NEW YORKER (June 10, 2013), http://www.newyorker.com/online/blogs/comment/2013/06/edward-snowden-nsa-leaker-is-no-hero.html.

[179] *Id.*

[180] *Fox News' Ralph Peters: 'Bring Back The Death Penalty' For Edward Snowden (VIDEO)*, THE HUFFINGTON POST (June 10, 2013), www.huffingtonpost.com/2013/06/10/edward-snowden-treason-fox-news_n_3416078.html.

[181] *Id.*

[182] EXEC. ORDER NO. 13,526, 75.2 C.F.R. 707 (2010).

[183] *Id.* §1.2(a)(1)–(3).

[184] Since the United States was founded in 1776, there has been only 21 years in which the U.S. was not engaged in any war. Danios, *"We're at War!" – And How We Have Been Since 1776: 214 Years of American War-Making*, LOONWATCH.COM (Dec. 20, 2011), http://www.loonwatch.com/2011/12/we-re-at-war-and-we-have-been-since-1776/.

information must be kept secret in order to advance our national security interests.[185] With this vast power comes great responsibility, and, as mentioned above, oftentimes the classification system is abused.

Accordingly, courts should look at the classified information to determine whether or not it is classified correctly. Professor Geoffrey Stone has provided an analytical framework that may prove helpful in a national security whistleblower context.[186] He argues that there are three types of government secrets: "illegitimate" government secrets; "legitimate but newsworthy" government secrets; and "legitimate and non-newsworthy" government secrets.[187] Using this framework, a court would be able to look at the confidentiality of the document while at the same time assessing the threat to national security. In theory, we should never punish a whistleblower who releases illegitimate secrets and always punish a whistleblower that falls under the third category.[188] Although the second category presents the more difficult task of scrutinizing those secrets that are legitimate, but newsworthy, it is a proper task for the court to undertake.

1. Illegitimate Government Secrets

"Illegitimate" secrets are those secrets that do nothing in any way to further the public good.[189] This often includes information that is made secret in an attempt to "hide an embarrassing or damning truth from public scrutiny."[190] This use of confidentiality runs afoul of democratic ideals of transparency, and must be exposed. Whistleblowers with access to these types of secrets are in a unique position. While the current law may discourage these whistleblowers from exposing any secrets,[191] it is vital in a constitutional democracy that such deception be fettered out and exposed.[192]

2. Legitimate But Newsworthy Government Secrets

As mentioned above, legitimate but newsworthy government secrets present the greatest challenge for a court. Obviously, the government has the right to keep things secret in order to protect national security. When these types of secrets are properly classified we can call them "legitimate." Yet, at the same time, exposing these "legitimate" secrets may also have salutary and substantial value as a step towards the truth.[193] When these types of secrets are involved, courts would then have to balance the national security interest against the public interest in obtaining the information.

---

[185] Presidents are right to protect information that might legitimately undermine national security or put Americans at risk. Radack & McClellan, *supra* note 101, at 102.

[186] Stone, *supra* note 143, at 95.

[187] *Id.*

[188] *Id.*

[189] *Id.* at 93-94.

[190] *Id.*

[191] *See* discussion *infra* Part II.

[192] Stone, *supra* note 143, at 93.

[193] *Id.*

A hypothetical scenario illustrates the conundrum. Suppose the government learns of inadequacies involving security at domestic nuclear power plants.[194] The government may definitely assert that exposure of this knowledge would present a threat to national security.[195] At the same time, the public would be interested in this material.[196] If the public knew, it would foster a healthy debate on the necessity to update security.[197] Unfortunately, these legitimate but newsworthy instances happen more often than not.[198] When confronted with this dilemma, courts should rule in favor of national security.

3. Legitimate and Non-Newsworthy Government Secrets

The third category involves those secrets which would harm national security if they were disclosed, and at the same time, contribute very little to informed public debate.[199] Determining whether or not information is non-newsworthy offers some additional challenges, but it is not an impossible test to overcome. A recent example would be the intelligence activities surrounding the raid on Osama bin Laden's compound in Pakistan. Everyone likely understood the absolute necessity to have kept secret the operation that found Osama bin Laden in order to catch him by surprise.[200] Keeping this information classified is therefore justified. At the same time, keeping the public in the dark was also justified because any exposed information may have led to bin Laden's escape. Accordingly, the information of intelligence activities surrounding the raid is properly classified as a "legitimate and non-newsworthy" secret.

4. The NSA's Telephony Metadata Program: Legitimate or Not?

When applying this factor to Snowden's case, a court may analyze this a few ways. First, it may rule on the underlying NSA program that has been disclosed. If the program is determined to be unconstitutional, keeping it secret would be "illegitimate." On the other hand, if the program is determined to be constitutional, it may qualify as a "legitimate" secret. Second, a court may also look at the national security risk disclosure poses. If that risk is substantial, keeping it secret may again be "legitimate."

Fortunately, two courts have recently ruled on the NSA telephony program's constitutionality, each reaching a different determination. On December 16, 2013, District Judge Richard J. Leon of the District of Columbia ruled that the NSA's bulk telephony metadata program may be unconstitutional.[201] He distinguishes *Smith v.*

---

[194] *Id.*

[195] *Id.*

[196] *Id.*

[197] *Id.*

[198] *Id.*

[199] *Id*. at 95.

[200] Moberly, *supra* note 54, at 114.

[201] Klayman v. Obama, 957 F. Supp. 2d 1, 9 (D.D.C. 2013) Judge Leon granted plaintiffs' preliminary injunction, holding that that plaintiffs "have demonstrated a substantial likelihood of success on the merits of their Fourth Amendment claim." *Id.* However, Judge Leon

Maryland,[202] a Supreme Court decision holding that individuals have no "legitimate expectation of privacy" regarding the telephone numbers they dial because they knowingly give that information to telephone companies when they dial a number.[203] Judge Leon opined that "present-day circumstances" have "become so thoroughly unlike those considered" in *Smith* that it does not apply to this case.[204] He found that the NSA surveillance techniques are much different than those employed in *Smith*,[205] the relationship between telecommunication providers and the government is much different than it was in *Smith*,[206] the ability of the government to analyze the metadata collected is much different,[207] and most importantly, the nature and quantity of the metadata is much greater and that people's cellphone habits nowadays indicate that they have a reasonable expectation of privacy.[208] Finding that a Fourth Amendment search took place in the case, Judge Leon held that there is a significant likelihood that plaintiffs will succeed in showing that the searches are unreasonable, and thus in violation of plaintiffs' Fourth Amendment rights.[209]

Just eleven days later, however, on December 27, 2013, District Judge William H. Pauley III of the Southern District of New York ruled that the exact same program was constitutional.[210] Unlike Judge Leon, Judge Pauley relied heavily on *Smith v. Maryland* to find that the NSA's telephony metadata program does not violate the Fourth Amendment.[211] Judge Pauley dismissed the ACLU's contention that the NSA's "telephony metadata program allows the creation of a rich mosaic," potentially revealing an individual's religious and political beliefs, contemplation of suicide, addictions to gambling or drugs, experience with rape, and grappling with sexuality[212] by stating:

> [A]t least three inflections from the Government's bulk telephony metadata collection [protect this from occurring]. First, without additional legal justification—subject to rigorous minimization procedures—the NSA cannot even query the telephony metadata base. Second, when it makes a query, it only learns the telephony metadata of the telephone

---

recognized significant national security interests at stake, so he stayed his order pending appeal. *Id.* at 10.

[202] Smith v. Maryland, 442 U.S. 735 (1979).

[203] *Id.* at 743.

[204] *Klayman*, 957 F. Supp. 2d at 31. Among these changes include how often citizens interact with their cellphones, the enormous reach of the NSA programs, and that the NSA program at issue is so different from the surveillance technique utilized in *Smith*. *Id.* at 32.

[205] *Id.* at 31.

[206] *Id.* at 33.

[207] *Id*. at 33.

[208] *Id*. at 34.

[209] *Id.* at 37.

[210] American Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 730 (S.D.N.Y. 2013).

[211] *Id.* at 752.

[212] *Id.* at 750.

> numbers within three "hops" of the "seed." Third, without resort to additional techniques, the Government does not know who any of the telephone numbers belong to.[213]

Furthermore, the phone records do not belong to the ACLU, but rather to Verizon or telephone providers.[214] Additionally, the NSA probing into that data is akin to FBI analysis of fingerprint data, which is perfectly constitutional.[215] Finally, Judge Pauley held that it "is unnecessary to decide whether there could be a First Amendment violation in the absence of a Fourth Amendment violation."[216]

As each Judge did the above cases, a court in Snowden's case must also look at the efficiency of the underlying program to determine whether or not keeping it a secret is "legitimate." As can be expected, both Judges came to different conclusions as to the effectiveness of the NSA's telephony metadata collection program. Judge Leon noted that there was an "utter lack of evidence that a terrorist attack has ever been prevented because the NSA database was faster than other investigative tactics," which led him to have "serious doubts about the efficacy of the metadata collection program."[217]

Judge Pauley on the other hand, believed that the "effectiveness of bulk telephony metadata collection cannot be seriously disputed."[218] He cited three specific examples of how the programs have led to information and the capture of terrorist suspects.[219] He also noted that these programs are not the only means to prevent terrorism, but rather significant tools in the grand goal of preventing terrorism.[220] Obviously, public officials agree with Judge Pauley, saying that "at least 50 threats . . .have been averted because of this information" worldwide.[221]

Independent research, however, has led to conclusions more in line with Judge Leon's misgivings about the program. One report, which analyzed 225 individuals associated with terrorists cells and charged in the United States with an act of terrorism since 9/11, concluded that the contribution of the "NSA's bulk surveillance programs…was minimal."[222] Rather, traditional investigative methods, "such as the use of informants, tips from local communities, and targeted intelligence operations," were the starting points for investigation in the majority of cases.[223]

---

[213] *Id.* at 750-51 (emphasis added).

[214] *Id.* at 751.

[215] *Id.*

[216] *Id.* at 753.

[217] Klayman v. Obama, 957 F. Supp. 2d 1, 40 (D.D.C. 2013).

[218] *Clapper*, 959 F. Supp. 2d at 755.

[219] *Id.* at 755-56.

[220] *Id.*

[221] Jackie Calmes, *Obama Says Surveillance Helped in Case in Germany*, N.Y. TIMES, June 20, 2013, at A6.

[222] Peter Bergen, et al., *Do NSA's Bulk Surveillance Programs Stop Terrorists?*, NEW AMERICAN FOUNDATION, Jan. 2014, at 1. The Report claims that the bulk telephony metadata program played an identifiable role in, at most, 1.8 percent of all these cases. *Id.* at 2.

[223] *Id.* at 1.

Another report referenced the examples Judge Pauley cited, and concluded that the bulk phone records collection did not make a significant contribution to stopping the terrorist plot.[224]

Review of the NSA bulk telephony metadata program's constitutionality and its efficacy in protecting national security leads this author to conclude that this type of secret should not be classified as "legitimate and non-newsworthy." While the constitutionality of the program is still being debated,[225] it is clear that the program does not produce the claimed results. Snowden, by exposing this program, did not disclose any information that would jeopardize national security. Rather, he provided the impetus to a worldwide debate concerning an invasive, yet largely inefficient surveillance program.

C. Third Factor—The Recipient of the Classified Information

As a third factor of the test, the court should take into account the recipient of the classified information. Clearly, if the recipient was a foreign government, weight of that fact would more easily contribute to a conviction. The scenario becomes more nuanced when the recipient is a media outlet. Below I highlight two media outlets – traditional news publishers and nontraditional news publishers. Whistleblowers who leak documents to traditional news publishers are more deserving of protection than those who leak the documents to nontraditional news publishers. The reasons for this conclusion are also highlighted below.

1. Traditional News Publishers

Traditional news publishers are press establishments like *The New York Times* and *The Washington Post*. Traditional news publishers have provided external restraints on government officials dating back to the American Revolution.[226] History reflects that these two institutions, the press and the government, have exhibited what some call a practice of "mutual restraint."[227] The basic idea of mutual restraint is the press "embraced an ethos of responsibility and the government generally treated leaks as an accepted, if not fully condoned, part of modern democratic governance."[228] The government rarely wants the information published, but together the two entities work out a solution. In turn, the government almost never attempts to block publishers from writing these stories.

---

[224] Marshall Erwin, *Connecting the Dots: Analysis of the Effectiveness of Bulk Phone Records Collection*, HOOVER INSTITUTION, Jan. 13, 2014, at 1.

[225] Both cases have been appealed. Klayman v. Obama, 957 F. Supp. 2d 1, *appeal docketed*, No. 13-00851 (D.C. Cir. Jan. 3, 2014); ACLU v. Clapper, 959 F. Supp. 2d 724, *appeal docketed*, No. 13-03994 (2d Cir. Jan. 2, 2014). It will be interesting to follow these cases in light of President Obama's January statements and the United States Supreme Court recent decision in *Riley v. California*, 573 U.S. __, 134 S. Ct. 2473 (2014) holding that law enforcement officials must obtain a search warrant prior to searching an arrestee's mobile device.

[226] Papandrea, *supra* note 17, at 257.

[227] McCraw & Gikow, *supra* note 12, at 473-74 (stating that "for the past forty years, this paradigm provided the framework for a political and legal reality most notable for the rarity of real conflict, in which the government and the press settled into an informal détente.").

[228] *Id.*

The *New York Times*' handling of the NSA wiretapping scandal highlighted an example of this mutual restraint. In the early 2000s, *The New York Times* learned of a classified program in which the NSA was monitoring phone calls that came into the United States from abroad.[229] The paper consulted with government officials who assured them that publication of this information would undermine an important tool in the fight against terrorism.[230] As a result, the *Times* held onto the story, and undertook its own research.[231] The *Times* finally published the information after extensive additional reporting whereby it concluded that the story would not provide useful information to terrorists.[232] This scenario reminds us that the "press has exercised remarkable self-restraint by routinely considering the ramifications of its publications and frequently holding stories or limiting their scope in order to soften their impact."[233]

2. Nontraditional News Publishers

Nontraditional publishers are "the product of new technology and new distribution channels, and they appear to be constrained only by the number of people willing to create them."[234] The prototypical example of these news publishers is WikiLeaks, which operates on the philosophy that it opens governments[235] to the public. It prides itself on being an online clearinghouse of confidential documents "in order to expose injustices in the world and try to rectify them."[236] Nontraditional publishers, such as WikiLeaks, present a legitimate threat to national security, government power, and the viability of mutual restraint.[237]

The Chelsea (f.k.a. Bradley) Manning case provided an example of this threat. In 2010, WikiLeaks announced that it possessed 251,287 cables originating from the U.S. State Department and 274 U.S. embassies and consulates around the world.[238] WikiLeaks began releasing this information in bits. The first bit involved 220 cables, which were also given to *The New York Times, The Guardian, Der Spiegel, Le Monde,* and *El Pais*.[239] The newspapers each consulted with the State Department in

---

[229] Papandrea, *supra* note 17, at 261.

[230] *Id.*

[231] *Id.*

[232] *Id.*

[233] *Id.* at 257.

[234] McCraw & Gikow, *supra* note 12, at 488.

[235] WIKILEAKS, http://wikileaks.org/ (last visited Nov. 6, 2013).

[236] McCraw & Gikow, *supra* note 12, at 488.

[237] *Id.*; *see also Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks: Hearing on H.R. 6506 Before the H. Comm. on the Judiciary*, 111th Cong. 14 (2010) (statement of Kenneth L. Wainstein, Partner, O'Melveny & Myers, LLP) *available at* http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg63081/html/CHRG-111hhrg63081.htm. WikiLeaks constitutes "an organization that is committed not to the traditional media function of reporting newsworthy information, but to the mass and indiscriminate disclosure of sensitive information.

[238] Bellia, *supra* note 36, at 1477.

[239] *Id.* at 1478.

order to redact certain information, such as the names of individuals who spoke privately with diplomats.[240] WikiLeaks originally did the same, releasing early sets of cables in redacted form.[241] Beginning in August 2011, however, WikiLeaks began releasing large batches of unredacted cables.[242]

In sum, the journalistic approaches advanced by traditional news publishers versus non-traditional news publishers vary significantly. While the traditional publishers conducted further reporting prior to publication, and decided to leave out names and other details after talking with government officials, WikiLeaks posted unredacted documents, exposing, among other things, the identities of foreign nationals in contact with U.S. embassies around the world.[243] Accordingly, leaks have a tremendous potential to cause significant damage when released to these non-traditional publishers rather than the traditional publishers.

As the above analysis demonstrates, the recipient of the leak must be factored into an analysis of the harm caused by the overall leak. Furthermore, it can provide an incentive to a would-be whistleblower to disclose the information to a traditional news publisher rather than a nontraditional news publisher.

3. *The Washington Post* and *The Guardian*: Twenty-First Century Traditional Publishers

Snowden disclosed the classified NSA telephony metadata collection program to two traditional news publishers: *The Washington Post* and British publisher *The Guardian*.[244] Both began publishing documents received from Snowden in early June 2013. Even in Snowden's case however, *The Washington Post* demonstrated responsible journalism by investigating further before printing the classified information. Among the documents leaked to these publishers were forty-one slides detailing specific NSA programs.[245] *The Washington Post* decided to only publish four of these slides.[246]

A few members of the press, however, are concerned with the journalistic approach advocated by Glenn Greenwald, Snowden's main contact at *The Guardian*.[247] In a conversation with Bill Smith of *The New York Times*, Greenwald

---

[240] *Id.*

[241] *Id.*

[242] *Id.*

[243] Downie, *supra* note 18.

[244] *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; *see also* Elliot & Rupar, *supra* note 128.

[245] Toobin, *supra* note 178.

[246] *Id.* Toobin argues this fact speaks to Snowden's irresponsibility when leaking these documents to the press. *Id.* While it is impossible to say with complete conviction whether or not the remainder of those slides would have harmed national security, this fact speaks to the importance of the traditional publisher. It is without doubt that nontraditional news publishers would have published every slide. The fact that the *Post* exercised its own discretion exemplifies why the recipient of the leak must be factored into the analysis.

[247] *See* Bill Keller, *Is Glenn Greenwald the Future of News?*, N.Y. TIMES (Oct. 27, 2013), http://www.nytimes.com/2013/10/28/opinion/a-conversation-in-lieu-of-a-column.html?src=rechp

argues that journalists must present their own opinions on news stories, and those opinions must be "grounded in facts, evidence, and verifiable data."[248] When it comes to publications that threaten national security, Greenwald argues that the "pre-publication process is both journalistically sensible . . . and legally wise."[249] He argues that he has done this for each article he has published concerning Snowden's NSA disclosures.[250] What he won't stand for is blind adherence to administrative wishes in the absence of any specific evidence or reason for journalistic suppression.[251]

The fact that Snowden disclosed the NSA information in this case to these two publishers may not have any impact on the current analysis. The information received was somewhat limited. When more information is disclosed, as in the Manning situation, the recipient may have a bigger impact on the analysis. As discussed above, traditional publishers tend to err on the side of caution and the protection of national security interests. That fact makes disclosures to these publishers more appealing, and calls for less severe punishment of those whistleblowers.

D. Fourth Factor—The Public Interest and Debate Sparked by the Leak

Under the fourth component of the test, two main issues must be reviewed: the public interest in the leak and the public debate sparked by the leak. These considerations allow a court to analyze two critical time periods: the time before the leak and the time after the leak.

1. Public Interest in the Leak

This element looks at the nature of the leak *before* exposure. It should be looked at objectively: "Would a reasonable, prudent citizen of the United States of America be interested in this material?" If the answer is yes, then the national security whistleblower is more justified in releasing the material. Again, a certain degree of transparency must be had in order to hold those in power accountable.[252] When those in power purposefully use the system to hide their transgressions, it is sometimes up to the courageous whistleblower to "air their dirty laundry."

United States v. Progressive, Inc.[253] is an illustrative example of public interest pre-leak. In *Progressive*, the magazine wished to publish "The H-Bomb Secret: How We Got It - - Why We're Telling It."[254] The Department of Energy ("DOE") argued that the article contained restricted information, and the court initially granted a temporary restraining order ("TRO").[255] The court reasoned that there was "no

---

&_r=0.

[248] *Id.*

[249] *Id.*

[250] *Id.*

[251] *Id.*

[252] Stone, *supra* note 21, at 3.

[253] United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979).

[254] Bejesky, *supra* note 51, at 450.

[255] *Id.*

plausible reason why the public needed to know the technical details about hydrogen bomb construction."[256]

While the initial TRO was eventually overturned,[257] the district court's rationale provides an interesting standard for the present test: Is there any plausible reason why the public would need to know the information? If so, a whistleblower would be justified in releasing this information.

2. Public Debate Sparked by the Leak

Courts often take into account what happens *down the road* from the crime[258] or the alleged wrongdoing.[259] This same analysis should apply to a national security setting. When confronted with a national security whistleblower, a court should first ask: Did any actual damage result from the leak? An affirmative answer would favor criminal charges; an answer in the negative would lead to acquittal.[260] The damage to national security must be real and actual, not a conglomerate of effects that leads to damage in theory. As mentioned above, embarrassment is not sufficient damage to national security so as to preclude disclosure.

A second question for a court to ask is whether the leak led to any meaningful public debate. A leak that did not result in any damage but did not lead to any meaningful debate or enhanced transparency is utterly useless and promotes disobedience. Leaks of this ilk would favor punishment. However, leaks that do not pose harm—such as the Pentagon Papers—or that meaningfully enhance transparency—like the disclosures of illegal operations—should not be a target for government sanction.[261] Placing an emphasis on the actual result of the leak would encourage leaks for the public benefit—resulting in the exposure of potential governmental abuses to the voters who then debate and determine how to react. A leak of this sort encourages the democratic ideals on which our government was founded.

3. Public Interest in the NSA Disclosures

a. Pre-Leak: The Front Page Test

Snowden's approach in determining whether or not to disseminate the classified information exemplifies the standard advocated above – "Is there any plausible reason why the public would need to know the information?" Snowden employed

---

[256] *Id.*

[257] *Id.*

[258] For example, a person severely injures another. The authorities apprehend the perpetrator, and charge him with assault. A few days later, the victim passes away. The defendant is then charged with murder, even though he intended only to assault his victim.

[259] The issue of damages is often looked at down the road in civil disputes. Yes, a defendant may have had a duty and may have breached that duty, but if the plaintiff can show no actual injury or any damages, the plaintiff is precluded from recovery.

[260] Of course the burden rests on the criminal defendant to prove by preponderance of the evidence that no damage to national security has occurred.

[261] McCraw & Gikow, *supra* note 12, at 498.

what he called "the front-page test" to determine interest in the information.[262] Beginning more than one-year prior to the leaks, Snowden began showing colleagues detailed maps which demonstrated the fact that the NSA was collecting more data on Americans in the United States than the Russian government collected on its people.[263] Snowden would then ask, "[w]hat do you think the public would do if this was on the front page?"[264]

The fact-finder must first try to forget about the present day effect the leaks had on society and put themselves into their own shoes before their leak. When that is done, the public interest in the programs Snowden disclosed seems overwhelming. While many may argue that the information disclosed was already known to the public,[265] it would be hard to argue the public knew the extent of the programs. It is very plausible that the public would take great interest in an Orwellian program designed to keep them safe.

b. Post-Leak

As stated above, a court must consider the actual result of the leak. First it must consider whether damage to national security occurred. While it may still be too early to determine, forecasts suggest that no damage to national security occurred in Snowden's case. As discussed above, the value to national security of the NSA's bulk metadata collection program was questionable prior to the disclosures.[266] It makes sense then that the damage to national security caused by his disclosure is minimal, if any. Furthermore, the fact that these disclosures may have embarrassed the United States government carries no significant weight. Government embarrassment is not a valid excuse for secrecy, and the government's embarrassment on the worldwide scale in this case should not be considered.

Second, a court must consider whether the leak led to any meaningful debate. As thoroughly demonstrated above, Snowden's actions have led to changes in public opinion as to national security and civil rights, demands for reform, proposed legislation, administrative change, and worldwide debate.[267] It is without question that Snowden's disclosures provided the catalyst to this debate. It is safe to say that Snowden's leak meaningfully enhanced transparency within our government, and furthered democratic ideals on which our country was founded.

IV. CONCLUSION

As Professor Patricia L. Bellia rightfully noted, factors like the sheer volume of information, the problem of overclassification, the breadth of access to information, and the ease of reproduction of information all make national security leaks more

---

[262] Barton Gellman, *Edward Snowden, After Months of NSA Revelations, Says His Mission's Accomplished*, WASH. POST (Dec. 23, 2013), http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html?hpid=z1.

[263] *Id.*

[264] *Id.*

[265] *See* Toobin, *supra* note 178.

[266] *See supra* notes 222-224 and accompanying text.

[267] *See supra* notes 4-6, 139-40.

likely to occur.[268] Additionally, as noted above, we cannot assume that all leaks are equal and that they will jeopardize national security.[269] Some provide significant benefits to society while others may cause severe harm. The proposed multi-factor test addresses these concerns by weighing the different set of facts provided in order to determine whether or not the national security whistleblower should be punished.

Whether or not one agrees with the application of these factors to Snowden's case is not the point of this paper. Rather, Snowden's case provided a timely scenario to exemplify how these factors may be applied to future national security whistleblowers. Edward Snowden will not be the last whistleblower our country and government encounters. More will follow. How we treat these individuals may determine the benefits that future leaks provide. A multi-factor test, like the one proposed, offers the whistleblower substantive protection while at the same time keeps secure national security interests.

[268] Bellia, *supra* note 36, at 1520.

[269] McCraw & Gikow, *supra* note 12, at 498.