

2017

Are Intelligence-Community Leakers Internationally Protected Whistleblowers or Simply “Whistling in the Dark”? Assessing the Protections Afforded to Intelligence-Community Whistleblowers Under International Law

Eric Connon

Follow this and additional works at: <https://scholarlycommons.law.case.edu/caselrev>

Recommended Citation

Eric Connon, *Are Intelligence-Community Leakers Internationally Protected Whistleblowers or Simply “Whistling in the Dark”? Assessing the Protections Afforded to Intelligence-Community Whistleblowers Under International Law*, 67 Case W. Res. L. Rev. 897 (2017)
Available at: <https://scholarlycommons.law.case.edu/caselrev/vol67/iss3/14>

This Note is brought to you for free and open access by the Student Journals at Case Western Reserve University School of Law Scholarly Commons. It has been accepted for inclusion in Case Western Reserve Law Review by an authorized administrator of Case Western Reserve University School of Law Scholarly Commons.

— Note —

ARE INTELLIGENCE-COMMUNITY
LEAKERS INTERNATIONALLY
PROTECTED WHISTLEBLOWERS OR
SIMPLY “WHISTLING IN THE DARK”?
ASSESSING THE PROTECTIONS
AFFORDED TO INTELLIGENCE-
COMMUNITY WHISTLEBLOWERS
UNDER INTERNATIONAL LAW

ABSTRACT

On June 9, 2013, the public discovered the source of the earthshattering stories revealing the full extent of the United States intelligence-gathering apparatus. Edward Snowden allowed the publication of his name and background at his own request because, as he claimed, “I know I have done nothing wrong.” This was the first public stage of the odyssey of Edward Snowden, whose quest for asylum or refugee status carried him from Hong Kong to a Moscow airport where, after failing to obtain secure passage to Latin American destinations, he was eventually granted asylum in Russia. Snowden found himself in a relative legal limbo, unable to gain asylum from most countries or safely access those countries that considered offering it. This Note analyzes the protection afforded under current international asylum and refugee law to intelligence community employees who leak information exposing perceived government misconduct. It also examines and considers the merits of possible means for improvement. While intelligence community whistleblowers may qualify as refugees or asylees based upon the political nature of their actions, the legal framework does not adequately address the situation in a consistent fashion. Alterations can and should be made to international refugee and asylum law, which would better protect good-faith intelligence community whistleblowers who expose government misconduct.

CONTENTS

INTRODUCTION: AN INTELLIGENCE COMMUNITY LEAKER’S SEARCH FOR ASYLUM	898
I. DEFINING “WHISTLEBLOWER” AT THE INTERNATIONAL LEVEL.....	905
A. <i>The Disclosure of Wrongdoings Connected to the Workplace</i>	910

B. A Public Interest Dimension, Such as “the Reporting of Criminal Offences, Unethical Practices, Rather Than a Personal Grievance”	911
C. Reporting of Wrongs through Designated Channels or Designated Persons	913
II. INTELLIGENCE-COMMUNITY WHISTLEBLOWERS UNDER EXISTING INTERNATIONAL LAW	918
A. Intelligence-Community Whistleblowers under Asylum Law	919
B. Intelligence Community Whistleblowers under the 1951 Convention Relating to the Status of Refugees and the 1967 Protocol	920
1. Meaning and Application of Well-Founded Fear	921
2. Does an Intelligence Community Whistleblower Fear “Persecution” Owing to One of the Enumerated Factors Listed in the Definition?	922
C. Is Intelligence-Community Whistleblowing a Political Act?	926
III. MEASURES TO IMPROVE PROTECTION OF INTELLIGENCE-COMMUNITY WHISTLEBLOWERS	929
A. Alterations to Domestic Law Whistleblower Protections	929
B. Alterations to International Law Whistleblower Protections	933
CONCLUSION: THE VALUE OF WHISTLEBLOWERS IN THE INTELLIGENCE COMMUNITY	936

INTRODUCTION: AN INTELLIGENCE COMMUNITY LEAKER’S SEARCH FOR ASYLUM

In June 2013, *The Guardian* published a series of groundbreaking articles revealing the unfettered access of the U.S. government to internet and phone records, either directly or through FISA¹ court-ordered acquisition of records held by private corporations.² The source

1. The Foreign Intelligence Service Court (“FISA”) was established under the Foreign Intelligence Service Act in 1978. *See generally* UNITED STATES FOREIGN SURVEILLANCE COURT, <http://www.fisc.uscourts.gov/> [<https://perma.cc/F7KB-CSY9>] (last visited Oct. 18, 2016) (“The Foreign Intelligence Surveillance Court was established by Congress in 1978. The Court entertains applications made by the United States Government for approval of electronic surveillance, physical search, and certain other forms of investigative actions for foreign intelligence purposes.”).

2. *See generally* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013, 6:05 AM), <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> [<https://perma.cc/NQC7-FBKY>] (revealing Verizon’s court-ordered relinquishment of millions of Americans’ phone records); Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

of these revelations was an unknown government contractor, Edward Snowden, who supplied this information to journalists from a hotel room in Hong Kong. As evidence, Snowden had four laptops in his possession containing, by one estimation, more than 1.5 million classified documents³ he accessed while employed by the National Security Agency ("NSA") in Hawaii.⁴ The release of Snowden's identity was not a mistake or the result of an investigation, but rather the intentional act of a man who considered himself to be, as conveyed by his journalist-contact Glenn Greenwald, a whistleblower.⁵ Snowden asserted, "I have no intention of hiding who I am because I know I have done nothing wrong."⁶ The Obama Administration, however, did not

[<https://perma.cc/5X8T-WMCL>] (describing the PRISM program, through which "[t]he National Security Agency and the FBI are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets . . ."); Glenn Greenwald & Ewen MacAskill, *Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data*, THE GUARDIAN (June 11, 2013, 9:00 AM), <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining> [<https://perma.cc/JR49-M49R>] (detailing the NSA tool, Boundless Informant, that allows the agency to record and analyze metadata and track, *inter alia*, the location or source of a piece of information).

3. H.R. PERMANENT SELECT COMM. ON INTELLIGENCE, EXECUTIVE SUMMARY OF REVIEW OF THE UNAUTHORIZED DISCLOSURES OF FORMER NATIONAL SECURITY AGENCY CONTRACTOR EDWARD SNOWDEN (2016) [hereinafter INTELLIGENCE COMMITTEE EXECUTIVE SUMMARY]. This number cited by the Intelligence Committee has been criticized in some quarters. See, e.g., Barton Gellman, *The House Intelligence Committee's Terrible, Horrible, Very Bad Snowden Report*, THE CENTURY FOUND. (Sept. 16, 2016), <https://tcf.org/content/commentary/house-intelligence-committees-terrible-horrible-bad-snowden-report/> [<https://perma.cc/8P53-L4KS>] ("In fact, the nation's most senior intelligence officers, no admirers of Snowden, have repeatedly said they can only surmise the number."); Trevor Timm, *The Washington Post is Wrong: Edward Snowden Should be Pardoned*, THE GUARDIAN (Sept. 19, 2016, 4:28 PM), <https://www.theguardian.com/commentisfree/2016/sep/19/washington-post-wrong-edward-snowden-pardon> [<https://perma.cc/DM84-CW7E>] ("Even the former NSA director himself admitted that the 1.5m number only represented the documents that Snowden 'touched', and officials didn't know how many he actually took.").
4. Glenn Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (June 11, 2013, 9:00 AM), <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance> [<https://perma.cc/TQN8-RENK>].
5. *Id.*
6. *Id.*

consider Snowden's public disclosures to constitute legitimate whistleblowing.⁷ On June 14, 2013, the U.S. government issued a complaint against Snowden⁸ for theft of government property⁹ and espionage.¹⁰ Congress also sent an official request to Hong Kong for his extradition.¹¹ Rather than return to the United States and face criminal sanction, Snowden instead cast about the international community for a safe haven.¹²

Though Snowden's subsequent transnational trek consisted only of a trip from Hong Kong to Moscow, it was accompanied by uncertainty, widespread media speculation, and heightened diplomatic stakes.¹³

-
7. See Aamer Madhani & David Jackson, *Obama: I Don't See Snowden as a Patriot*, USA TODAY (Aug. 9, 2013, 9:20 PM), <http://www.usatoday.com/story/news/politics/2013/08/09/obama-news-conference/2636191/> [<https://perma.cc/C2YA-HFL6>] (“[Obama] said Snowden’s leaks, which have come out in dribs and drabs, have unfairly set the impression that the U.S. government is spying on its citizens.”).
 8. Criminal Complaint, United States v. Snowden, No. 1:13 CR 265, (E.D. Va. June 14, 2013).
 9. 18 U.S.C. 641 (2012) (“Whoever . . . steals . . . or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record . . . of the United States or of any department or agency thereof . . . [s]hall be fined under this title or imprisoned not more than ten years, or both . . .”).
 10. 18 U.S.C. 793(d) (2012) (prescribing penalties for unauthorized collection and communication of national defense information); 18 U.S.C. 798(a)(3) (2012) (prohibiting willful communication of “intelligence activities of the United States” to an unauthorized person); see also Criminal Complaint, *supra* note 8 (charging Snowden with violations of: “18 U.S.C. 641[,] Theft of Government Property[.]” “18 U.S.C. 793(d)[.] Unauthorized Communication of National Defense Information[.]” and “18 U.S.C. 798(a)(3)[.] Willful Communication of Classified Communications Intelligence Information to an Unauthorized Person”).
 11. Mirren Gidda, *Edward Snowden and the NSA Files—Timeline*, THE GUARDIAN (Aug. 21, 2013, 5:54 PM), <http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline> [<https://perma.cc/GP2M-ZXE3>].
 12. Haroon Siddique, *Edward Snowden Asylum: Countries Approached and Their Responses*, THE GUARDIAN (July 4, 2013, 11:38 AM), <http://www.theguardian.com/world/2013/jul/02/edward-snowden-nsa-asylum-application-list-countries> [<https://perma.cc/DHJ3-V2T4>] (citing Snowden’s statement that he had applied for asylum in a total of 21 countries to that date).
 13. See, e.g., Michael Pearson, Matt Smith & Jethro Mullen, *Snowden’s Asylum Options Dwindle*, CNN (July 2, 2013, 7:15 PM), <http://www.cnn.com/2013/07/02/politics/nsa-leak/> [<https://perma.cc/QX49-BNWW>] (describing Snowden’s limited options).

Snowden checked out of his Hong Kong hotel room on June 14th and disappeared until June 23rd, when he boarded a flight to Moscow.¹⁴

Snowden faced substantial hurdles in his efforts to resist extradition and secure safe passage to a country willing to grant asylum. He had intended for Moscow to be a temporary layover to allow for a connecting flight to Cuba, but the U.S. government derailed that plan by cancelling Snowden's passport, preventing further international travel.¹⁵ He found himself stranded in Sheremetyevo Airport, applying for asylum status in more than twenty countries, including China, Austria, Finland, India, Spain, and Switzerland.¹⁶ Bolivia, Ecuador, Nicaragua, and Venezuela offered him permanent asylum, but Snowden chose to apply for temporary asylum in Russia because of concerns that he could not access a safe, direct route to one of those four countries from Moscow.¹⁷ Russia declined to extradite Snowden to the United States and, instead, granted him a one-year temporary asylum,¹⁸ which Russia extended for three more years in the summer of 2014.¹⁹

Edward Snowden's case illustrates the challenging predicament for intelligence-community employees²⁰ who leak information exposing perceived government misconduct. Though many government employees

14. *Id.*

15. *Id.*

16. Siddique, *supra* note 12 (including European countries such as Iceland, Italy, Ireland, Norway, and Poland).

17. Phil Black, Laura Smith-Spark & Michael Martinez, *Snowden Meets with Rights Groups, Seeks Temporary Asylum in Russia*, CNN (July 13, 2013, 9:29 AM), <http://www.cnn.com/2013/07/12/world/europe/russia-us-snowden/> [<https://perma.cc/K6H2-RBDS>]; see also Emily C. Kendall, Note, *Sanctuary in the 21st Century: The Unique Asylum Exception to the Extradition Rule*, 23 MICH. ST. INT'L L. REV. 153, 170 (2014) ("Four countries offered him *permanent* asylum: Bolivia, Ecuador, Nicaragua, and Venezuela. However, Mr. Snowden chose to apply for temporary asylum in Russia because he did not feel he would be able to safely travel to any Latin American country, since Bolivian President Evo Morales's flight from Russia to Bolivia had been rerouted and denied airspace in France, Spain, and Italy due to suspicions that Mr. Snowden was on board." (emphasis in original) (citations omitted)).

18. Steven Lee Myers & Andrew E. Kramer, *Defiant Russia Grants Snowden Year's Asylum*, N.Y. TIMES (Aug. 1, 2013), <http://www.nytimes.com/2013/08/02/world/europe/edward-snowden-russia.html?> [<https://perma.cc/23XB-FBFT>].

19. Isabel Gorst, *Russia Gives Edward Snowden Asylum for Three More Years*, L.A. TIMES (Aug. 7, 2014, 10:37 AM), <http://www.latimes.com/world/europe/la-fg-russia-snowden-asylum-20140807-story.html> [<https://perma.cc/J5W8-3UYD>].

20. The focus of this Note is on the employees of agencies and governmental departments (including employees of contractors for those bodies) whose

or contractors may wish to challenge what they perceive as unethical, illegal, or corrupt practices within the workplace, many do not have the legal and institutional protections needed to come forward safely.²¹ Depending on the nature of the information disclosed, attempts to bring complaints and revelations to the press can result in criminal charges.²² Snowden's case is noteworthy because, unlike other intelligence-community leakers,²³ he evaded domestic law enforcement and entered the international legal realm.

Snowden's travails reveal much about the current protections afforded to intelligence-community leakers under domestic and international law. Should Edward Snowden and other leakers be classified as whistleblowers, deserving of protection under domestic whistleblower laws? If not, do they instead qualify for the extraterritorial protections afforded to refugees or asylees under international law? If the leakers do constitute whistleblowers, but are denied safe harbor under both domestic and international law, what can or should be done to better address and protect those employees and contractors exposing government misconduct?

"principal function [is] conducting foreign intelligence or counterintelligence activities," including, but not limited to, the Central Intelligence Agency, Defense Intelligence Agency, National Imagery and Mapping Agency, National Reconnaissance Office, National Security Agency, and Federal Bureau of Investigation. See RODNEY M. PERRY, CONG. RESEARCH SERV., R43765, INTELLIGENCE WHISTLEBLOWER PROTECTIONS: IN BRIEF 2 (2014) (citations omitted) (describing the agencies covered by intelligence agency whistleblower statutes).

21. Simon Wolfe, Mark Worth, Suelette Dreyfus & A J Brown, *Whistleblower Protection Rules in G20 Countries: The Next Action Plan*, BLUEPRINT FOR FREE SPEECH 1, 21 (2014), https://www.griffith.edu.au/__data/assets/pdf_file/0010/619075/Whistleblower-Protection-Rules-in-G20-Countries-The-Next-Action-Plan-June-2014.pdf [<https://perma.cc/P5DZ-TVG4>] (indicating that only two G20 countries have "very/quite comprehensive provisions outlining what procedures public sector organizations must put in place").
22. *Id.* at 59 (noting the U.S. government's prosecution of intelligence-community leakers such as Thomas Drake, John Kiriakou, Bradley Manning, and Edward Snowden).
23. This Note uses the word "leaker" with regard to the high profile intelligence-community figures discussed within, including Edward Snowden. There is considerable debate as to whether those figures constitute legitimate whistleblowers and the standard use of the term "whistleblower" presupposes their legal status. See Dana Farrington, *What is Meant by the Term 'Whistleblower'*, NPR (June 10, 2013, 1:38 PM), <http://www.npr.org/sections/thetwo-way/2013/06/10/190380255/what-we-mean-when-we-say-whistleblower> [<https://perma.cc/G9LQ-GGPW>] (discussing the use of the term whistleblower with regard to Edward Snowden and NPR's decision to instead use the term "leaker" in its reporting).

This Note will explore the actions of intelligence-community leakers and the available safeguards afforded under domestic and international law. If, as is frequently the case, intelligence-community leakers are not properly shielded by domestic whistleblower legislation, it is also unlikely that they would qualify for protection as refugees or asylees under international law. Because of the gaps in protection afforded to intelligence-community employees, modifications to existing whistleblower legal frameworks are needed at both the domestic and international levels to both encourage reporting of government wrongdoing and to limit the frequency and extent of large-scale public disclosures.

Part I will consider whether intelligence-community leakers constitute whistleblowers. Despite regional and national variances, a functional international definition for "whistleblower" can be gleaned from the major analyses comparing best practices for whistleblower legislation generally and the intelligence community more specifically. This definition can then serve to assess the whistleblower status of several high-profile intelligence-community leakers.

Part II will consider the position of intelligence-community leakers under the two separate frameworks of refugee and asylum law. If unable to qualify for whistleblower protection under domestic law, would intelligence-community leakers nevertheless qualify as refugees sufficient to trigger the protections of the 1951 Convention Relating to the Status of Refugees²⁴ and the 1967 Protocol Relating to the Status of Refugees?²⁵ If not, do intelligence-community leakers have a sufficient legal basis to resist extradition through the political offense exception within extradition treaties, a staple of asylum law generally?²⁶ The answers to these questions serve to assess whether intelligence-community leakers qualify for protection under existing international law.

Part III explores possible alterations to intelligence-community whistleblower protection. The suggested changes can be grouped into two layers of protection: front-end (domestic) and back-end (international) protections.²⁷

24. Convention Relating to the Status of Refugees, art. 1, July 28, 1951, 189 U.N.T.S. 137 [hereinafter Refugee Convention].

25. Protocol Relating to the Status of Refugees art. 1, Jan. 31, 1967, 606 U.N.T.S. 267 [hereinafter 1967 Protocol]. Although related to the Refugee Convention, the 1967 Protocol is technically an independent instrument.

26. Christine van den Wijngaert, *The Political Offence Exception to Extradition: Defining the Issues and Searching a Feasible Alternative*, 17 REVUE BELGE DE DROIT INT'L 741, 741 (1983) (suggesting universal acceptance of the political offense exception "can be deduced from the fact that almost every extradition law and treaty contains the rule . . .").

27. This Note uses the terms "front-end" and "back-end" solely for characterizing the two layers (domestic and international) of possible whistleblower protections. The terms should not be equated or confused with their common

In terms of front-end protections, there are several modifications to domestic whistleblower legal frameworks that would encourage intelligence-community whistleblowing while limiting the frequency and extent of large-scale public disclosures. First, states should establish a governmental body with greater independence from the executive branch to handle whistleblower complaints. Potential intelligence-community whistleblowers should also be provided with streamlined access to intelligence oversight bodies, in which any communications are kept confidential from the whistleblower's superiors. Lastly, public disclosure should be retained as an option for intelligence-community whistleblowers if the internal mechanisms for disclosure have been exhausted, but with a high threshold necessary to qualify. Such a threshold would allow for public disclosure in the event of institutional failure to address misconduct or illegality, but would protect necessary government secrets through strict requirements that whistleblowers first utilize available internal reporting mechanisms.

The back-end, or international approaches, would protect intelligence-community whistleblowers in the event that domestic whistleblower protections are lacking or misapplied. There are two possible avenues to enhance intelligence-community whistleblower protection at the international level.

The first, more ambitious approach would focus on the creation of a new international instrument such as a treaty or convention. While the proposed Snowden Treaty²⁸ is an intriguing first step put forth by advocates of intelligence-community whistleblowers, it is redundant in its privacy protections and is unlikely to receive widespread acceptance.

A slightly less ambitious model would involve creating a government whistleblowing protocol along the lines of the 1967 Protocol. This new international tool would entail adding a defined 'government whistleblower' category to those protected under the 1951 Convention,²⁹ which would afford protection to those fearing

usage in the web industry. For information on the latter usage, *see, e.g.*, Ivan Codesido, *What is Front-End Development?*, THE GUARDIAN (Sept. 28, 2009, 12:59 PM), <http://www.theguardian.com/help/insideguardian/2009/sep/28/blogpost> [<https://perma.cc/7H94-56CH>] (describing the Internet discipline of "[f]ront-end or client-side development").

28. *The Snowden Treaty: A New International Treaty on the Right to Privacy, Protection Against Improper Surveillance and Protection of Whistleblowers*, http://media.wix.com/ugd/fb845b_89e20fe385844f348fbc79a6ede39a4d.pdf [<https://perma.cc/8L8D-7XVT>] [hereinafter *The Snowden Treaty*].

29. Refugee Convention, *supra* note 24, at art. I(A)(2) (defining refugee as one who, "owing to well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his nationality and is unable or, owing to such fear, is unwilling to avail himself of the protection of that country").

persecution for exposing government misconduct. Such a protocol could include a third-party adjudicator, such as the United Nations High Commissioner on Refugees ("UNHCR"), to decide the status of government whistleblowers. A neutral arbiter could solve the common diplomatic and political influence that plagues the refugee or asylee determination process and prevents consistent application of refugee and asylum law. Even this less ambitious model, however, would likely face obstacles similar to those confronting a new treaty.

The second, more modest approach would work within the existing international conventions as currently formulated. Under this second scenario, the UNHCR would adjust the guidelines and Handbook³⁰ to recommend clearer and enhanced protections for a narrowly-defined set of government whistleblowers under the 1951 Convention and the 1967 Protocol. It would also consist of intensive encouragement of states to adopt the whistleblower guidelines of the G20 Whistleblower Study³¹ and the more narrowly tailored Tshwane Principles,³² which address the unique situation of intelligence-community whistleblowers. Lastly, the guidelines would require that the judiciary, not the executive, determine the refugee or asylee status of applicants.

Collectively, improvements to domestic and international legal regimes would begin to address obstacles encountered by intelligence-community whistleblowers in their endeavors to report employer wrongdoing.

I. DEFINING "WHISTLEBLOWER" AT THE INTERNATIONAL LEVEL

If refugee or asylum law protections extend to intelligence-community leakers, a uniform definition of whistleblower is an essential

-
30. UNITED NATIONS HIGH COMM'R ON REFUGEES, HANDBOOK ON PROCEDURES AND CRITERIA FOR DETERMINING REFUGEE STATUS (1979, reissued 2011), <http://www.unhcr.org/en-us/publications/legal/3d58e13b4/handbook-procedures-criteria-determining-refugee-status-under-1951-convention.html?query=handbook> [<https://perma.cc/TP97-FBJC>] [hereinafter UNHCR HANDBOOK].
 31. OECD, G20 ANTI-CORRUPTION ACTION PLAN, PROTECTION OF WHISTLEBLOWERS: STUDY ON WHISTLEBLOWER PROTECTION FRAMEWORKS, COMPENDIUM OF BEST PRACTICES AND GUIDING PRINCIPLES FOR LEGISLATION (2011), <http://www.oecd.org/g20/topics/anti-corruption/48972967.pdf> [<https://perma.cc/BDG4-B5Q2>] [hereinafter G20 WHISTLEBLOWER STUDY].
 32. OPEN SOC'Y FOUNDS., THE GLOBAL PRINCIPLES ON NAT'L SEC. AND THE RIGHT TO INFO. (TSHWANE PRINCIPLES) (2013), <https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf> [<https://perma.cc/PN9V-4XB9>] [hereinafter TSHWANE PRINCIPLES].

first step to determining what individuals qualify under existing international legal frameworks. Arriving at a common definition for whistleblower at the international level is a challenging endeavor, however, because there “is no common legal definition of what constitutes whistleblowing[.]”³³ at least as applied by states through domestic legislation.

There are many statutory regimes containing whistleblower protections. The global community has included whistleblower protections in a number of international instruments aimed at curbing corruption.³⁴ Whistleblower legislation is also present at the state level, which can often feature overlapping, fragmented laws that provide varying degrees of protection for different categories of whistleblowers.³⁵ The United States, for instance, provides whistleblower protection at both the state³⁶ and federal level,³⁷ but with a multitude of critical distinctions

33. G20 WHISTLEBLOWER STUDY, *supra* note 31, at 7.

34. *See, e.g.*, United Nations Convention Against Corruption, arts. 8, 13 & 33, Dec. 9, 2003, G.A. Res. 58/4 (Oct. 30, 2004) (encouraging the implementation of legal and regulatory measures to protect those seeking to report corruption); Organization of American States, Inter-American Convention against Corruption, art. III(8), Mar. 29, 1996, S. Treaty Doc. No. 105-39, 35 I.L.M. 724 (same); OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, arts. IX, X(C)(v), Dec. 17, 1997, (encouraging the implementation of legal and regulatory measures to protect those seeking to report bribery of foreign public officials).

35. *See* ANJA OSTERHAUS & CRAIG FAGAN, TRANSPARENCY INT’L, ALTERNATIVE TO SILENCE: WHISTLEBLOWER PROTECTION IN 10 EUROPEAN COUNTRIES 3-4 (2d ed. 2009) (finding whistleblowing legislation in the ten countries researched was “generally fragmented and weakly enforced” with “no single, comprehensive legislative framework in place, with the exception of Romania”).

36. *See* Gerard Sinzdek, Comment, *An Analysis of Current Whistleblower Laws: Defending a More Flexible Approach to Reporting Requirements*, 96 CALIF. L. REV. 1633, 1641 (2008) (“Whistleblower statutes are available in some form in every state.”) (citation omitted).

37. *See, e.g.*, Whistleblower Protection Act of 1989, Pub. L. No. 101-12, 103 Stat. 16 (codified as amended in scattered sections of 5 U.S.C. (2012)) (strengthening protections for Federal employees seeking to report violations of law, gross waste, mismanagement, and abuse); Act of Oct. 29, 1994, Pub. L. No. 103-424, 108 Stat. 4361 (codified as amended in scattered sections of 5 U.S.C. (2012)) (same); False Claims Amendments Act of 1986, 31 U.S.C. §§ 3729-3733 (2012) (providing procedures and rewards for civil lawsuit whistleblowers under the False Claims Act); Clean Air Act Amendments of 1977, 42 U.S.C. § 7622 (2012) (outlining protections, procedures, and remedies for employees who report employer’s violations of the Clean Air Act); Energy Policy Act of 1992, 42 U.S.C. § 5851 (2012) (strengthening protections for employees seeking to report violations of the Atomic Energy Act of 1954); Housing and Community Development Act of 1992, 31 U.S.C. § 5328 (2006) (outlining protections and remedies for employees seeking to

within those statutes and regulations with regard to the definition of protected whistleblowing.

The discrepancies among whistleblower laws lie in the substance of what is reported, the categories of people covered by the protections, and the procedural requirements of protected whistleblowing. Of these elements, the widest variations lie in the procedural requirements employees must follow to qualify for protected whistleblower status. U.S. state whistleblower statutes differ, *inter alia*, with regard to whether employees are required to provide prior notice to supervisors before alerting oversight bodies³⁸ as well as the degree to which employees must be informed of whistleblowing procedures.³⁹ Viewed

report employer's violations of the Act); National Defense Authorization Act for Fiscal Year 1987, 10 U.S.C. § 2409 (2012) (protecting employees of federal contractors and subcontractors seeking to report gross mismanagement, fraud, abuse, and dangers to public health and safety); Federal Mine Safety and Health Act of 1977, 30 U.S.C. § 815(c) (2012) (outlining protections, procedures, and remedies for employees seeking to report violations concerning health and safety in mine operations); Federal Water Pollution Control Act Amendments of 1972, 33 U.S.C. § 1367 (outlining protections, procedures and remedies for employees seeking to report violations of federal laws under the Act); Sarbanes-Oxley Act of 2002, 18 U.S.C. § 1514A (outlining protections, procedures, and remedies for employees of publicly traded companies seeking to report the company's violations of federal laws and regulations).

38. *See, e.g.*, KAN. STAT. ANN. § 75-2973(d)(2) (Supp. 2015) ("No supervisor or appointing authority of any state agency shall . . . require any such employee to give notice to the supervisor or appointing authority prior to making any such report."); KY. REV. STAT. ANN. § 61.102(1) (LexisNexis 2015) ("No employer shall require any employee to give notice prior to making such a report, disclosure, or divulgence."). *But see* ME. STAT. tit. 26 § 833(2) (2016) ("Subsection 1 does not apply to an employee who has reported or caused to be reported a violation . . . unless the employee has first brought the alleged violation, condition, or practice to the attention of a person having supervisory authority with the employer and has allowed the employer a reasonable opportunity to correct that violation, condition or practice.").
39. *See, e.g.*, W. VA. CODE ANN. § 6C-1-8 (LexisNexis 2015) ("An employer shall post notices and use other appropriate means to notify employees and keep them informed of protections and obligations set forth in the provisions of this article."); KAN. STAT. ANN. § 75-2973(g) (Supp. 2015) ("Each state agency shall prominently post a copy of this act in locations where it can reasonably be expected to come to the attention of all employees of the state agency."); N.H. REV. STAT. ANN. § 275-E:7 (2010) ("Every employer shall post such notices as are prescribed by the commissioner of labor as a means of keeping such employer's employees informed of their protections and obligations under this chapter. The commissioner of labor shall adopt rules, under RSA 541-A, relative to the form, content, and placement of such notices.").

collectively, whistleblower laws vary markedly and exist at the international, national, and local levels.

Potential whistleblowers from within the intelligence community face additional procedural restrictions due to the sensitive nature of the information handled.⁴⁰ In the United States, the Whistleblower Protection Act,⁴¹ which governs whistleblower protections for federal employees, “expressly excluded intelligence agency employees from its applicability.”⁴² To address this, Congress passed the Intelligence Community Whistleblower Protection Act of 1998 (“WPA”),⁴³ which enabled employees of agencies “to report to Congress a matter of urgent concern.”⁴⁴ The protections for intelligence-community whistleblowers against retaliatory measures were further modified by Presidential Policy Directive 19⁴⁵ and Title VI of the Intelligence Authorization Act for Fiscal Year 2014 (Title VI),⁴⁶ which ostensibly protect intelligence-community whistleblowers from reprisal.⁴⁷ Collectively, the three measures protect certain forms of disclosures, but employees are rigidly constrained in available reporting channels.⁴⁸ These reporting channels

-
40. See G20 WHISTLEBLOWER STUDY, *supra* note 31, at 9 (“Some whistleblower protection laws expressly exclude . . . those in the intelligence services or the army[.]” while in several other countries, “public sector employees who are engaged in particularly sensitive areas of work may be subject to a special whistleblower protection legislation.”).
41. Whistleblower Protection Act of 1989, Pub. L. No. 101-12, 103 Stat. 16 (1989) (codified as amended in scattered sections of 5 U.S.C.).
42. PERRY, *supra* note 20, at 1.
43. Pub. L. No. 105-272, 112 Stat. 2413 (1998) (codified as amended in scattered sections of 5 U.S.C. and 50 U.S.C.).
44. Daniel D’Isidoro, *Protecting Whistleblowers and Secrets in the Intelligence Community*, HARV. NAT. SEC. J. (Sep. 29, 2014, 9:01 PM), <http://harvardnsj.org/2014/09/protecting-whistleblowers-and-secrets-in-the-intelligence-community/> [https://perma.cc/TRM5-3REN].
45. Presidential Policy Directive/PPD-19: Protecting Whistleblowers with Access to Classified Information (Oct. 10, 2012).
46. Pub. L. No. 113-126, 128 Stat. 1390, 1414 (2014) (codified as amended in scattered sections of 50 U.S.C.).
47. *Making Lawful Disclosures*, OFFICE OF THE DIRECTOR OF NAT’L INTELLIGENCE, <https://www.dni.gov/index.php/about-this-site/contact-the-ig/making-lawful-disclosures> [https://perma.cc/QM2R-WGAC] (last visited Sept. 5, 2016).
48. Mieke Eoyang, *Should Intelligence Whistleblowers Be Protected?*, THE ATLANTIC (Jan. 23, 2016), <https://www.theatlantic.com/politics/archive/2016/01/should-intelligence-whistleblowers-be-protected/424872/> [https://perma.cc/674E-QVR6]. Unlike employees in “most agencies” who “can bring their concerns straight to the [congressional] committees[.]” intelligence-community employees must first report to their agency Inspector General,

“do not include disclosures to media sources”⁴⁹ and would not protect the government leakers under consideration in this Note.

Despite the variations between statutes, a working definition of whistleblower can be ascertained through two analyses that compare best practices and common characteristics and, in one case, consider the unique circumstances of intelligence-community whistleblowers.

The first of these two resources is the compendium of the best practices in whistleblower protection drafted by the G20 Anti-Corruption Working Group (“G20 Whistleblower Study”).⁵⁰ In it, the Working Group identified several key characteristics common to whistleblowing: (1) “the disclosure of wrongdoings connected to the workplace”; (2) “a public interest dimension, *e.g.* the reporting of criminal offences, unethical practices, etc., rather than a personal grievance”; and (3) “the reporting of wrongdoings through designated channels and/or designated persons.”⁵¹ The G20 list is generally applicable to all manner of whistleblowers within both the private and public spheres.

Those three listed elements should be analyzed in conjunction with the more specific, intelligence-community whistleblower definitional components contained in the second resource, the Tshwane Principles.⁵² The Tshwane Principles were a collaborative, two-year effort of twenty-two groups and 500 experts, which provides “guidance to those engaged in drafting, revising, or implementing laws or provisions relating to the state’s authority . . . to punish the disclosure of [national security] information.”⁵³ The resulting comparison between the two resources reveals a working definition for intelligence-community whistleblowers that may prove sufficiently acceptable at the international level.

“who forwards the complaint to the agency head, who decides whether to notify Congress.” *Id.* Intelligence-community employees “may contact the committees directly if the [Inspector General] overrules them or forwards incorrect information[.]” but even in that case “the employee must notify the agency head and abide by any security procedures the agency head imposes.” *Id.*

49. PERRY, *supra* note 20, at 1.

50. G20 WHISTLEBLOWER STUDY, *supra* note 31.

51. *Id.* ¶ 15.

52. TSHWANE PRINCIPLES, *supra* note 32, at 49–56.

53. *Id.* at 5.

A. *The Disclosure of Wrongdoings Connected to the Workplace*

The more general definition of wrongdoing offered in the G20 Whistleblower Study is concise and does not add precise detail into what constitutes a “wrongdoing” that would merit disclosure.⁵⁴

For intelligence-community whistleblowers, a suspected wrongdoing may range from trivial to treasonous in severity. Both the Whistleblower Protection Act and the Tshwane Principles offer broadly defined meanings for what constitutes a “wrongdoing” with several subcategories. The Whistleblower Protection Act protects employees who report an “urgent concern,” which includes a “false statement to Congress” as well as “a serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to the funding, administration, or operations of an intelligence activity . . . but does not include differences of opinions concerning public policy matters.”⁵⁵ The Tshwane Principles provide an 11-category list of wrongdoing characterized as a “protected disclosure” if revealed.⁵⁶ The enumerated list includes criminal offenses, human rights and international humanitarian law violations, corruption, dangers to public health and safety, dangers to the environment, abuse of public office, miscarriages of justice, mismanagement or waste of resources, retaliation for disclosure of wrongdoing offenses, and “deliberate concealment of any matter falling into one of the above categories.”⁵⁷

One fear with such a broad definition is that it would allow low-level employees to become “the ultimate arbiter of what is right and wrong” with a country’s policies.⁵⁸ These low-level employees, notably Edward Snowden and Chelsea Manning, released records with which, in many cases, the “leakers admit to having had little or no familiarity.”⁵⁹ That broad policy can place government employees with access

54. See G20 WHISTLEBLOWER STUDY, *supra* note 31, at 9 (“Some countries set minimum thresholds on the extent of the wrongdoing before whistleblower protection may be triggered.”).

55. Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, § 702(a)(G)(i)(I)–(II), 112 Stat. 2413, 2415 (codified as amended at 50 U.S.C. §. 3517 (d)(5)(G)(i)(I)–(II) (2012)).

56. TSHWANE PRINCIPLES, *supra* note 32, at 49.

57. *Id.*

58. Steven Bucci, *Edward Snowden Broke the Law: Opposing View*, USA TODAY (June 10, 2013, 8:32 PM), <http://www.usatoday.com/story/opinion/2013/06/10/edward-snowden-heritage-foundation-editorials-debates/2410213/> [<https://perma.cc/7TRJ-Y3SF>].

59. Margaret B. Kwoka, *Leaking and Legitimacy*, 48 U.C. DAVIS L. REV. 1387, 1401 (2015).

to classified information in challenging situations to judge the constitutionality of employers' behavior.⁶⁰

The examples provided, although expansive, give an indication of the types of employer or supervisor misconduct that prompt employees to report. The absence of narrowly tailored categories of wrongdoing is tempered, however, by the third element within the G20 Whistleblower Study—the use of internal, designated channels and personnel to receive whistleblowing complaints.⁶¹ Consequently, a broad meaning of wrongdoing can encourage government employees to report all manner of suspicious activity, while the filtering mechanism of internal channels can forestall any deluge of complaints to outside third parties.

B. A Public Interest Dimension, Such as "the Reporting of Criminal Offences, Unethical Practices, Rather Than a Personal Grievance"

The motivation of a whistleblower in making a disclosure is a key concern for determining the level of protection merited. Especially as it pertains to government employees in possession of classified information, the motivation may well prove the difference between a disclosure's characterization as whistleblowing or traitorous.⁶²

The G20 Whistleblower Study notes that "[a] principal requirement in most whistleblower protection legislation is that the disclosures be made in 'good faith' and on 'reasonable grounds.'"⁶³ In its guiding principles, the study defines a "good faith" disclosure as a report made "based upon the individual's reasonable belief that the information disclosed evidenced one of the identified conditions in the statute, even if

60. PEN AMERICAN CENTER, SECRET SOURCES: WHISTLEBLOWERS, NATIONAL SECURITY, AND FREE EXPRESSION 13 (2015), <http://www.pen.org/sites/default/files/Sekret%20Sources%20report.pdf> [<https://perma.cc/BCZ8-S4WP>] [hereinafter SECRET SOURCES] (stating that the U.S. executive director for intelligence community whistleblowing explained that he would have told a pre-disclosure Snowden that it is "nice you think [the mass surveillance programs are] unconstitutional, but staking your career on your hypothetical opinion about constitutionality is very dangerous").

61. See *infra* Part I.C (discussing internal reporting channels).

62. See Jo Becker, Adam Goldman, Michael S. Schmidt & Matt Apuzzo, *N.S.A. Contractor Arrested in Possible New Theft of Secrets*, N.Y. TIMES (Oct. 5, 2016), http://www.nytimes.com/2016/10/06/us/nsa-leak-booze-allen-hamilton.html?_r=0 [<https://perma.cc/3ACL-KUL4>] (stating that, while investigators did not think the investigation against arrested National Security Agency contractor Harold T. Martin looked "like a traditional espionage case," an official noted that "investigators thought that [Mr. Martin] was not politically motivated—not like a Snowden or someone who believes that what we were doing was illegal and wanted to publicize that").

63. G20 WHISTLEBLOWER STUDY, *supra* note 31, at 8.

the individual's belief is incorrect."⁶⁴ The activities disclosed should have a public interest basis, meaning the activities "threaten[] or pose[] a risk to others."⁶⁵ Conversely, a disclosure should not be motivated by a personal grievance, centered on "the staff member's own employment position" and which has no bearing on others.⁶⁶

To that end, whistleblower protection laws afford no protection to individuals that make "false disclosures" even though many governing bodies overseeing whistleblowing disclosures "would normally not impose sanctions for misguided reporting, and . . . disclosures that are made in honest error."⁶⁷ This conception is in line with the Tshwane Principles, which note that, as long as the disclosure relates to a listed wrongdoing and is not "knowingly untrue" when made, the motivation "is irrelevant."⁶⁸ Both definitions afford protection to good-faith disclosures of wrongdoing with a public interest dimension.

In very high profile examples of public disclosures by intelligence-community employees, the motivations appear to comport with this element. For example, Edward Snowden—in his own words—sought to "inform the public as to that which is done in their name and that which is done against them."⁶⁹ He did not appear to "possess a profit motive," nor did he appear motivated by "personal gain or the gain of others."⁷⁰ Former NSA administrator Thomas Drake was motivated to disclose publicly his concerns that "the government's eavesdroppers were squandering hundreds of millions of dollars on failed programs while ignoring a promising alternative."⁷¹ Former CIA analyst John Kiriakou was driven to publicly disclose his "concerns about the [CIA's] use of enhanced interrogation techniques and waterboarding."⁷² In leaking hundreds of thousands of classified documents to WikiLeaks,

64. *Id.* at 31.

65. *Frequently Asked Questions*, NHS EMPLOYERS (Nov. 4, 2014), <http://www.nhsemployers.org/case-studies-and-resources/2014/04/frequently-asked-questions> [<https://perma.cc/WPT4-7BLF>].

66. *Id.*

67. G20 WHISTLEBLOWER STUDY, *supra* note 31, at 8.

68. TSHWANE PRINCIPLES, *supra* note 32, at 50.

69. Greenwald et al., *supra* note 4.

70. Mark D. Kielsgard & Ken Gee-Kin Ip, *Hong Kong's Failure to Extradite Edward Snowden: More than Just a Technical Defect*, 13 RICH. J. GLOBAL L. & BUS. 49, 62 (2014).

71. Scott Shane, *Obama Takes a Hard Line Against Leaks to Press*, N.Y. TIMES (June 11, 2010), <http://www.nytimes.com/2010/06/12/us/politics/12leak.html> [<https://perma.cc/UK9G-RQMB>].

72. SECRET SOURCES, *supra* note 60, at 13.

Chelsea Manning wished to “‘make the world a better place’ and spark a national debate over the military’s role in U.S. foreign policy.”⁷³

Though some analysts have warned that sanctioning public disclosure of classified materials could allow employees to “take it upon themselves to sabotage the programs they don’t like[,]”⁷⁴ the motivations of the intelligence-community leakers cited above comport to the public interest element of the G20 definition. Though many people “have more than one motivation to act[,]”⁷⁵ the evidence indicates that the leakers profiled above were in large part motivated by public interest concerns—exposing government wrongdoing or waste affecting the nation as a whole.⁷⁶

*C. Reporting of Wrongdoings through Designated Channels
or Designated Persons*

One of the most challenging elements for potential intelligence-community whistleblowers to meet is the requirement that disclosures first proceed through designated channels or persons. A frequent complaint leveled against intelligence-community leakers disclosing mass surveillance and enhanced interrogation programs to the press is that those employees who suspect wrongdoing have alternate, legitimate means to bring concerns to supervisors and Congress “without breaking the law.”⁷⁷

President Barack Obama remarked that “[t]here were other avenues available for someone [like Edward Snowden,] ‘whose conscience felt stirred.’”⁷⁸ Indeed, Obama noted that he “signed an executive order well before Mr. Snowden leaked this information that provided whistleblower protection to the intelligence community for the first time.”⁷⁹

73. Janet Reitman, *Bradley Manning Explains His Motives*, ROLLING STONE (Feb. 28, 2013), <https://www.rollingstone.com/politics/news/bradley-manning-explains-his-motives-20130228> [<https://perma.cc/79D4-3UKX>] (quoting from Manning’s 35-page statement).

74. Jeffrey Toobin, *Edward Snowden Is No Hero*, THE NEW YORKER (June 10, 2013), <http://www.newyorker.com/news/daily-comment/edward-snowden-is-no-hero> [<https://perma.cc/YX34-KCG8>].

75. Kwoka, *supra* note 59, at 1396.

76. See Eoyang, *supra* note 48 (“Michael Horowitz, the IG for the Department of Justice, recently stated that 80 percent of whistleblowers are motivated to improve the system, not tear it down.”).

77. Bucci, *supra* note 58.

78. Madhani & Jackson, *supra* note 7.

79. Editorial, *Edward Snowden, Whistle-Blower*, N.Y. TIMES (Jan. 1, 2014), <https://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html?> [<https://perma.cc/X8DL-ZAM6>]. Hillary Clinton also argued that Snowden should have internally reported his concerns, suggesting that

The Intelligence Community Whistleblower Protection Act of 1998, moreover, provides that the whistleblower should “notify the agency head, through an Inspector General, before they can report an ‘urgent’ concern to a congressional intelligence committee.”⁸⁰ If the prosecuted government leakers had an adequate internal channel to disclose concerns, then whistleblower protection could be unwarranted in the event of public disclosure.

However, though an internal channel exists statutorily, it may not be an effective means to counteract wrongdoing or the correcting office may have no interest in addressing the complaint. Though John Kiriakou chose not to use internal reporting mechanisms, he refrained because “he believed he ‘wouldn’t have gotten anywhere’ as his superiors and the congressional intelligence committees were already aware of the program.”⁸¹ Because the law did not provide an alternate channel for external disclosure, the U.S. government indicted Kiriakou after his disclosures to the press.⁸²

Thomas Drake took his concerns about the government’s eavesdropping programs “everywhere inside the secret world: to his bosses, to the agency’s inspector general, to the Defense Department’s inspector general and to the Congressional intelligence committees[,] [b]ut he felt his message was not getting through.”⁸³ An investigation by the Inspector General’s (“IG”) office of the Department of Defense “substantially affirmed” Drake’s complaint and forwarded the findings to the House and Senate committees overseeing the NSA.⁸⁴ Despite this, once the subject of his complaint was published in the *New York Times*,

“[h]e could have gotten all of the protections of being a whistleblower.” Mark Hertsgaard, *How the Pentagon Punished NSA Whistleblowers*, THE GUARDIAN (May 22, 2016, 10:00 AM), <https://www.theguardian.com/us-news/2016/may/22/how-pentagon-punished-nsa-whistleblowers> [<https://perma.cc/V7WF-9ZNN>].

80. SECRET SOURCES, *supra* note 60, at 13; Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, § 702(a)(D)(i)–(ii), 112 Stat. 2413, 2414 (codified as amended at 50 U.S.C. § 3517 (d)(5)(D)(i)–(ii) (2012)).
81. SECRET SOURCES, *supra* note 60, at 13 (quoting Interview with John Kiriakou (Aug. 4, 2015)).
82. Wolfe et al., *supra* note 21, at 59.
83. Shane, *supra* note 71. When Drake “told his boss, Baginski, that the NSA’s expanded surveillance following 9/11 seemed legally dubious, she reportedly told him to drop the issue: the White House had ruled otherwise.” Hertsgaard, *supra* note 79.
84. Hertsgaard, *supra* note 79. The whistleblower complaint joined by Drake “helped nudge Congress to end funding for” a wasteful government program named Trailblazer. *Id.*

senior Defense Department officials repeatedly broke the law to persecute Drake.⁸⁵ These officials, according to John Crane, the former assistant inspector general at the IG's office, "revealed Drake's identity to the Justice Department[,] . . . withheld (and perhaps destroyed) evidence after Drake was indicted[, and then] lied about all this to a federal judge."⁸⁶

Edward Snowden did not attempt to report within the designated channel, but there were valid reasons for his failure to disclose internally. If Snowden had attempted to raise his concerns with Congress or the NSA Inspector General, he may not have found a receptive audience because "differences of opinions concerning public policy matters" is not characterized as an "urgent concern" warranting public disclosure, and in any event, "the law would not have protected him from retaliatory employment action for having done so."⁸⁷ Moreover, Snowden was aware of the fate that befell Drake and the other potential intelligence-community whistleblowers.⁸⁸ Snowden characterized what he understood to be the value of the NSA's internal whistleblowing channels in the following critique:

Name one whistleblower from the intelligence community whose disclosures led to real change—overturning laws, ending policies—who didn't face retaliation as a result. The protections just aren't there The sad reality of today's policies is that going to the inspector general with evidence of truly serious wrongdoing is often a mistake.⁸⁹

Nevertheless, Snowden claims "he brought his misgivings to two superiors in the NSA's Technology Directorate and two more in the NSA Threat Operations Center."⁹⁰ Faced with maintaining silence or sacrificing his career without impacting the source of his concern, Snowden

85. *Id.*

86. *Id.*

87. SECRET SOURCES, *supra* note 60, at 15.

88. See Hertsgaard, *supra* note 79 (quoting Snowden as remarking in 2015 that "[i]t's fair to say that if there hadn't been a Thomas Drake, there wouldn't have been an Edward Snowden").

89. *Id.*

90. Barton Gellman, *Edward Snowden, After Months of NSA Revelations, Says His Mission's Accomplished*, WASH. POST (Dec. 23, 2013), https://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 [https://perma.cc/8ETQ-FRED] (responding to critical accusations that he did not pursue internal channels of dissent, Snowden replied, "[h]ow is that not reporting it? How is that not raising it?").

pursued a risky third alternative—public disclosure to the press. As he explained, “[g]oing to the press involves serious risks, but at least you’ve got a chance.”⁹¹

Because an unauthorized disclosure “is ‘prohibited by law’ and will not be afforded whistleblower protection unless it is made to the agency’s Inspector General or the Office of Special Counsel[.]”⁹² Snowden made arrangements to flee the country in advance of his public disclosure.⁹³ Fully cognizant that prior whistleblowers often could not substantiate their allegations “because the government had classified all the evidence[.]” Snowden also “took the evidence with him” in the form of thousands of NSA documents.⁹⁴

Because not all internal channels for whistleblowing disclosures are sufficiently responsive, consideration of the reporting context must be afforded to whistleblowers who fail to follow or disregard the internal disclosure mandates of their employers and instead take their concerns to the media. The Tshwane Principles protects disclosures to the public in the following circumstances:

[T]he body to which the disclosure was made refused or failed to investigate the disclosure effectively . . . [; or] [t]he person reasonably believed that there was a significant risk that making the disclosure internally . . . would have resulted in the destruction or concealment of evidence, interference with a witness, or retaliation against the person or a third party; [or] there was no established internal body or independent oversight body to which a disclosure could have been made.⁹⁵

An important caveat in the Tshwane Principles, however, is the requirement that the potential whistleblower “only disclose[] the amount of information that [is] reasonably necessary to bring to light the wrongdoing.”⁹⁶ Critics of Snowden—even those that concede he performed a measure of public service in his disclosure—assert that his acts went beyond whistleblowing because a large portion of the material he stole and revealed compromised lawful, needed government programs.⁹⁷ This was the opinion of the House Intelligence Committee,

91. Hertzgaard, *supra* note 79.

92. G20 WHISTLEBLOWER STUDY, *supra* note 31, at 10.

93. Greenwald et al., *supra* note 4.

94. Hertzgaard, *supra* note 79 (emphasis omitted).

95. TSHWANE PRINCIPLES, *supra* note 32, at 51–52.

96. *Id.* at 52.

97. See, e.g., Fred Kaplan, *The Leaky Myths of Snowden*, SLATE (Sept. 16, 2016, 4:40 PM), https://www.slate.com/articles/news_and_politics/war_stories/2016/09/what_snowden_gets_wrong_about_its_hero.html [https:

which argued that “Snowden caused tremendous damage to national security, and the vast majority of the documents he stole have nothing to do with programs impacting individual privacy interests”⁹⁸ Snowden supporters counter that he took precautions to reveal only what was reasonably necessary, noting that “[i]nstead of dumping a mass of documents on the internet, he gave them to experienced national security reporters [and] relied on their judgments about what was in the public interest.”⁹⁹ The fear that potential whistleblowers that go to the public may reveal too much is a legitimate concern. As explained by Michael Horowitz, the IG for the Department of Justice, “because normal whistleblower protections do not shield government employees who run straight to the media, those who do so may go for broke, taking as much information as possible.”¹⁰⁰

Governmental departments and agencies, especially those in the intelligence communities and others working with sensitive, classified information, should certainly have internal reporting channels that employees can resort to for whistleblowing disclosures. Nevertheless, those same governmental bodies should ensure that the internal bodies provide more than just superficial lip service to employee concerns. As the Tshwane Principles aptly describe, the internal body should “investigate the alleged wrongdoing and take prompt measures with a view to resolving the matters . . . [or] refer it to a body that is authorized

[//perma.cc/RHQ7-2CPW](https://perma.cc/RHQ7-2CPW)] (“The fact is, many of Snowden’s documents [that he seized] bore no resemblance to whistleblowing as the phrase is broadly understood.” Many of the activities revealed “are legitimate aspects of the NSA’s charter, which involves intercepting communications of foreign powers. They have nothing to do with domestic surveillance or spying on allies.”); Editorial, *No Pardon for Edward Snowden*, WASH. POST (Sept. 17, 2016), https://www.washingtonpost.com/opinions/edward-snowden-doesnt-deserve-a-pardon/2016/09/17/ec04d448-7c2e-11e6-ac8e-cf8e0dd91dc7_story.html [<https://perma.cc/KML5-MYRS>] (“[Snowden] also pilfered, and leaked, information about a separate overseas NSA Internet-monitoring program, PRISM, that was both clearly legal and not clearly threatening to privacy Worse—far worse—he also leaked details of basically defensible international intelligence operations”).

98. INTELLIGENCE COMMITTEE EXECUTIVE SUMMARY, *supra* note 3, at 1 (emphasis omitted).
99. Trevor Timm, *The Washington Post Is Wrong: Edward Snowden Should Be Pardoned*, THE GUARDIAN (Sept. 19, 2016, 4:28 PM), <https://www.theguardian.com/commentisfree/2016/sep/19/washington-post-wrong-edward-snowden-pardon> [<https://perma.cc/3NHB-HVW3>]. Those reporters charged with filtering and disseminating Snowden’s documents “allowed the government to make objections (some of which they listened to) tied to national security concerns.” *Id.*
100. Eoyang, *supra* note 48.

and competent to investigate.”¹⁰¹ If those elements are not present, governments should not retaliate against whistleblowers who reasonably perceive no option other than public disclosure. In providing this public reporting avenue, however, officials could then require a potential whistleblower to limit public disclosure to that necessary to expose the wrongdoing.

II. INTELLIGENCE-COMMUNITY WHISTLEBLOWERS UNDER EXISTING INTERNATIONAL LAW

The intelligence-community leakers described above failed to find protection under domestic whistleblowing legislation. Should those same leakers have found protection under international law? Edward Snowden is a useful test case to assess whether intelligence community whistleblowers qualify for protected status under existing international law. This is because, unlike the other intelligence-community leakers discussed previously, he escaped domestic law enforcement and sought the protection of the international community.

Whistleblowers could conceivably find protection under international refugee law or asylum law. International refugee law is rooted in the 1951 Convention Relating to the Status of Refugees¹⁰² and the 1967 Protocol Relating to the Status of Refugees.¹⁰³ In asylum law—which is customary international law and based on the principle of non-refoulement—states may refuse to extradite asylees to a requesting state by citing a “political offence” exception, a component of almost every bilateral extradition treaty.¹⁰⁴ A political offense exception involves an act that is either “directed solely against the political order . . . [or] directed at both the political order and private rights.”¹⁰⁵

An analysis of both the Refugee Convention and asylum law reveals that a national security whistleblower’s status under either legal framework comes down to one essential question—does whistleblowing constitute a political act or political opinion? Persecution based on political belief stands as the only viable protected category within the definition of “refugee” that could widely apply to national security

101. TSHWANE PRINCIPLES, *supra* note 32, at 51.

102. Refugee Convention, *supra* note 24.

103. 1967 Protocol, *supra* note 25.

104. Van den Wijngaert, *supra* note 26, at 741.

105. Christine E. Cervasio, Comment, *Extradition and the International Criminal Court: The Future of the Political Offense Doctrine*, 11 PACE INT’L L. REV. 419, 426 (1999).

whistleblowers under international refugee law.¹⁰⁶ Because the political offense exception under asylum law considers whether an act was political in its effect and motivation, the key determining factor is the same under both legal frameworks. Answering whether intelligence-community whistleblowing constitutes a political act will therefore determine what, if any, protections are afforded to those whistleblowers under current international law.

Under both refugee law and the asylum law, it is the state in which the applicant applies for protection that determines the applicant's potential refugee or asylee status. The Refugee Convention allows government officials in the state of application to determine refugee status,¹⁰⁷ while under asylum law, the decision as to whether an act qualifies for the political offense exception is taken "unilaterally" by the state of application.¹⁰⁸ Because the definitions of refugees or political offense asylees are vaguely written or entirely absent in some cases, the decisions are nearly always politically influenced and subject to state discretion.¹⁰⁹

A. Intelligence-Community Whistleblowers under Asylum Law

Asylum law has ancient roots and entails the conditions "under which a foreign sovereign or religious order may accept a person seeking protection from persecution in his home country."¹¹⁰ Asylum law is situated within the larger context of bilateral extradition agreements between states, which detail "the legal process by which a foreign country delivers a fleeing citizen to his home country upon request from the home country."¹¹¹ While extradition agreements are designed to "contractually prevent" a treaty partner's offer of asylum to the requesting

106. See Refugee Convention, *supra* note 24, at art. 1(A)(2) (listing the categories protected under refugee law as "race, religion, nationality, membership of a particular social group or political opinion").

107. UNHCR HANDBOOK, *supra* note 30, ¶ 189.

108. Van den Wijngaert, *supra* note 26, at 744.

109. *Id.* ("[E]xtradition laws and treaties almost never define the term political offence, and consequently, the definition is unvariably a matter of judicial interpretation and administrative discretion."); see also UNHCR HANDBOOK, *supra* note 30, ¶ 191 (explaining that because refugee determination is left to the contracting states, the procedures utilized "vary considerably" from state to state.).

110. Kendall, *supra* note 17, at 154 (citation omitted).

111. *Id.* (citation omitted); see also *id.* at 158 (noting that "the U.S. maintained extradition treaties with more than 100 countries including Australia, Ecuador, Spain, Canada, Colombia, the United Kingdom, Kenya, Liberia, and Iraq").

state's nationals,¹¹² the political offense exception remains a commonly cited loophole. If an asylee can convince his host state that his alleged offense was political in nature, the state could resist an extradition request, even if an extradition treaty is in force.¹¹³

The political offense exception is "one of the most universally accepted and one of the most universally contested rules of international law."¹¹⁴ The political offense exception and asylum law generally remain in the exclusive purview of the specific states party to an extradition agreement,¹¹⁵ which has resulted in incongruous application internationally. Each country has developed its own conception of political offense "with the result that the question as to whether a crime is political or non-political may be differently answered from one state to another."¹¹⁶ As with the international refugee law, a leaker's protected status under asylum law will depend on whether intelligence community whistleblowing is viewed as a political act by the requested state. If so, that state could cite a political offense exception in resisting extradition.

*B. Intelligence Community Whistleblowers under the 1951 Convention
Relating to the Status of Refugees and the 1967 Protocol*

Though subject to state determination, refugee characteristics are nonetheless given a definition under the Refugee Convention.¹¹⁷ The Refugee Convention consolidates previous international agreements and international norms relating to refugees and "provides the most comprehensive codification of the rights of refugees at the international level."¹¹⁸ As of April 2015, there are 142 states party to both the original 1951 Convention and the 1967 Protocol.¹¹⁹ Those qualifying as refugees

112. *Id.* at 154.

113. Van den Wijngaert, *supra* note 26, at 750–51 (noting that some extradition agreements now contain depoliticization—essentially exceptions to the political offense exception—wherein "a given offence will not be considered political for the purposes of extradition").

114. *Id.* at 741.

115. *Id.* at 744 ("[T]he decision as to whether or not a given offence qualifies as political is taken unilaterally by the requested State.").

116. *Id.*

117. Refugee Convention, *supra* note 24, at art. 1(A).

118. U.N. HIGH COMM'R FOR REFUGEES, *Introductory Note to CONVENTION AND PROTOCOL RELATING TO THE STATUS OF REFUGEES 3* (2010), <https://www.unhcr.org/3b66c2aa10.html> [<https://perma.cc/SS62-HAMR>].

119. U.N. HIGH COMM'R FOR REFUGEES, *STATES PARTIES TO THE 1951 CONVENTION RELATING TO THE STATUS OF REFUGEES AND THE 1967*

under the Refugee Convention cannot be forcefully “expel[led] or return[ed] . . . to the frontiers of territories where his life or freedom would be threatened.”¹²⁰ If an intelligence-community whistleblower qualified as a refugee, a state would be precluded from expelling or returning him to his country of origin.

The key question, then, is whether Snowden or other intelligence-community leakers would qualify as refugees under the Refugee Convention. Refugees are those possessing a “well-founded fear of being persecuted [by their country of nationality] for reasons of race, religion, nationality, membership of a particular social group or political opinion.”¹²¹ The definition as it pertains to whistleblowers can be approached by considering two factors: (1) the meaning and application of a “well-founded fear;” and (2) does an applicant fear “persecution” owing to one of the enumerated factors listed in the definition?

1. Meaning and Application of Well-Founded Fear

The key to determining whether an intelligence-community whistleblower could be subjected to persecution is a “well-founded fear.” There are two parts to this phrase—one being subjective and the other being an objective, reasonableness standard. As the UNHCR notes, “fear is subjective” and, as it will vary from person to person, a determination of a given refugee’s fear should be measured first by the applicant’s statement and frame of mind.¹²² People display and reveal fear in different manners, and this subjective element must consider the applicant’s personal level of fear.

The second component of the phrase is an objective, reasonableness standard. The applicant’s frame of mind must be supported by an objective situation—“[f]ear must be reasonable” and not “[e]xaggerated.”¹²³ This part of determining an applicant’s fear should consider his background, personal experiences, and the situation in the country of origin. The UNHCR states that an applicant’s fear “should be considered well-founded if he can establish, to a reasonable degree, that his continued stay in his country of origin has become intolerable to him for the reasons stated in the definition, or would for the same reasons be intolerable if he returned there.”¹²⁴ In determining whether an

PROTOCOL 1 (2008), <https://www.unhcr.org/3b73b0d63.html> [<https://perma.cc/2BJU-9BDS>].

120. Refugee Convention, *supra* note 24, at art. 33(1).

121. *Id.* at art. 1(A)(2).

122. UNHCR HANDBOOK, *supra* note 30, ¶¶ 37–38.

123. *Id.* ¶ 41.

124. *Id.* ¶ 42.

applicant has well-founded fear, both the subjective and the objective elements must be met.¹²⁵

In the case of Edward Snowden, there was clear evidence of a subjective fear on his part. When considering the U.S. government's reaction, Snowden remarked, "[y]es, I could be rendered by the CIA. I could have people come after me . . . that is a concern I will live with for the rest of my life, however long that happens to be."¹²⁶ Snowden's fear is evidenced not only by his words, but by his actions. Glenn Greenwald noted that, while in his Hong Kong hotel room, Snowden "line[d] the door of his hotel room with pillows to prevent eavesdropping," and put "a large red hood over his head and laptop when entering his passwords to prevent any hidden cameras from detecting them."¹²⁷ Snowden clearly met the subjective element, as his fear of U.S. government reprisal was evident to those around him.

As far as the objective, reasonable element of the test, Snowden's fear was well-founded. The United States had charged Snowden with three felonies, including two under the 1917 Espionage Act, which could send him to prison "for decades if not life upon conviction."¹²⁸ By revealing the classified information to the media, Snowden faced, at the minimum, an extensive prison sentence. This deprivation of liberty, whether justified or not, would certainly constitute a well-founded fear as it would be "intolerable" for Snowden to remain or return to the United States when facing the prison sentence. Snowden and other intelligence-community whistleblowers would likely meet the elements of the first factor and demonstrate a well-founded fear of U.S. government reprisals.

2. Does an Intelligence Community Whistleblower Fear "Persecution"
Owing to One of the Enumerated Factors Listed in the Definition?

To qualify as a refugee, Snowden would need to have a well-founded fear of persecution. Do the possible U.S. reprisals constitute persecution under the Refugee Convention, and is the alleged persecution tied to one of the factors listed within the Refugee Convention's definition?

Persecution has a potentially broad meaning. In the opinion of two noted scholars, the "core meaning" of persecution "readily includes the

125. *Id.* ¶ 38.

126. Greenwald et al., *supra* note 4. Snowden went so far as to speculate that the CIA could employ the Triads to seize him. *Id.*

127. *Id.*

128. Glenn Greenwald, *On the Espionage Act Charges Against Edward Snowden*, THE GUARDIAN (June 22, 2013), <https://www.theguardian.com/commentisfree/2013/jun/22/snowden-espionage-charges> [<https://perma.cc/9TEH-YZGR>].

threat of deprivation of life or physical freedom.”¹²⁹ This is a potentially expansive definition, but one that “remains very much a question of degree and proportion.”¹³⁰ The deprivation of physical freedom that is the *sine-qua-non* of prison sentences could potentially constitute persecution if it was tied into the enumerated rationales listed within the Refugee Convention.

For a prison sentence to constitute persecution under the Refugee Convention, it must be based on or the result of discrimination or mistreatment related to an applicant’s “race, religion, nationality, membership of a particular social group or political opinion.”¹³¹ In the case of Snowden and other potential whistleblowers, the first three may be dispensed with quickly. Any potential persecution of Edward Snowden was not tied to his race, religion, or nationality. The prison sentence imposed by the U.S. government would result from Snowden’s seizure and disclosure of classified government documents.

Snowden could assert that government whistleblowers are part of a particular social group, though such a conception is unlikely to gain traction within the international community. The UNHCR notes that “a ‘particular social group’ normally comprises persons of similar background, habits or social status” and “may be at the root of persecution because there is no confidence in the group’s loyalty to the Government or because the political outlook . . . of its members, or the very existence of the social group as such, is held to be an obstacle to the Government’s policies.”¹³² From that broader definition, government whistleblowers could potentially qualify as a particular social group. The “members” of the group have a similar background as government employees with first-hand familiarity with the inner workings of the U.S. government. Furthermore, it is conceivable that the U.S. government might question the loyalty of government whistleblowers or consider the existence of the group as a threat to the government’s policies. Certainly, Snowden has been characterized as a traitor,¹³³ and his

129. GUY S. GOODWIN-GILL & JANE MCADAM, *THE REFUGEE IN INTERNATIONAL LAW* 92 (2007).

130. *Id.*

131. Refugee Convention, *supra* note 24, at art. 33(1).

132. UNHCR HANDBOOK, *supra* note 30, ¶¶ 77–78.

133. *See, e.g.*, Elise Foley, *Michael Hayden ‘Drifting’ Toward Calling Edward Snowden a ‘Traitor,’* HUFFINGTON POST (Dec. 29, 2013, 12:32 PM), http://www.huffingtonpost.com/2013/12/29/michael-hayden-edward-snowden_n_4515705.html [<https://perma.cc/EP5T-DVK6>] (quoting former Director of the NSA Michael Hayden, in describing Edward Snowden, as saying he is now “drifting in the direction of perhaps more harsh language . . . such as ‘traitor’”).

disclosure of the inner-workings of the U.S. intelligence apparatus has been characterized as a threat to government security.¹³⁴

The key point against Snowden is that not all government whistleblowers fit within that category. The government encourages and rewards certain forms of whistleblowing against government misconduct.¹³⁵ However, perhaps the “particular social group” could be more narrowly defined as whistleblowers that expose misconduct within the classified intelligence community. A stronger case could be made for persecution of that group, as the Obama administration has conducted seven prosecutions of leakers under the Espionage Act, which is “more than double the number under all prior US presidents combined.”¹³⁶ It may be possible to conceive of government whistleblowers that use classified materials to expose government misconduct as a social group.

Nevertheless, intelligence-community whistleblowers would be unlikely to prevail in arguments that their collective acts result in the creation of a social group in line with the Refugee Convention’s language. In 2002, the UNHCR issued further guidance and a clarified definition of a particular social group as a “group of persons who share a common characteristic other than their risk of being persecuted, or who are perceived as a group by society. The characteristic will often be one which is innate, unchangeable, or which is otherwise fundamental to identity, conscience or the exercise of one’s human rights.”¹³⁷

134. See, e.g., John Bolton, *Edward Snowden’s Leaks are a Grave Threat to US National Security*, THE GUARDIAN (June 18, 2013), <http://www.theguardian.com/commentisfree/2013/jun/18/edward-snowden-leaks-grave-threat> [<https://perma.cc/6JHH-FPPM>] (comparing Snowden’s disclosures to “Benedict Arnold scheming to betray West Point’s defenses to the British”).

135. See Whistleblower Protection Act of 1989, Pub. L. No. 101-12, 103 Stat. 16, 16 (codified as amended in scattered sections of 5 U.S.C.) (recognizing that whistleblower disclosures can “serve the public interest by assisting in the elimination of fraud, waste, abuse, and unnecessary Government expenditures”).

136. Greenwald, *supra* note 128 (emphasis omitted). Taking a more combative stance than the previous administration, the Trump White House has vowed to more actively pursue and prosecute leakers from within the law enforcement and intelligence agencies. See Julie Hirschfeld Davis, *Trump Denounces F.B.I. Over Leaks, Demanding Investigation*, N.Y. TIMES (Feb. 24, 2017), <https://www.nytimes.com/2017/02/24/us/politics/trump-fbi-leaks.html> [<https://perma.cc/XVJ6-JC5Z>] (noting that “President Trump . . . assailed the F.B.I. as a dangerously porous agency, charging that leaks of classified information from within its ranks were putting the country at risk—and calling for an immediate hunt for the leakers”).

137. U.N. High Comm’r for Refugees, *Guidelines on International Protection: “Membership of a Particular Social Group” Within the Context of Article 1A(2) of the 1951 Convention and/or its 1967 Protocol Relating to the*

There are two steps within this definition to determine whether a refugee is a member of a particular social group under the Refugee Convention. One must first determine if the shared characteristic of the group is immutable—is it a feature that “cannot be changed” or, though possible to change, “ought not . . . be required to be changed because they are so closely linked to the identity of the person or are an expression of fundamental human rights.”¹³⁸ The second step is to consider whether the group is “socially perceived and cognizable.”¹³⁹

The first step can be dealt with swiftly—it would be a great leap to consider government whistleblowing an immutable characteristic that is “linked to the identity of the person.”¹⁴⁰ The UNHCR Social Group Guidelines did note that shopkeepers or members of a particular profession might constitute a particular social group “if in the society they are recognized as a group which sets them apart.”¹⁴¹ The government whistleblowers have certainly garnered a great deal of public attention and media reports have occasionally linked intelligence-community whistleblowers together.¹⁴² Yet it is unlikely that society sees these whistleblowers within the intelligence community as a distinct, cognizable group.¹⁴³ Because of the unlikelihood that intelligence-

Status of Refugees, ¶ 11, U.N. Doc. HCR/GIP/02/02 (May 7, 2002) [hereinafter UNHCR Social Group Guidelines].

138. *Id.* ¶ 12.

139. Isaac T.R. Smith, Note, *Searching for Consistency in Asylum's Protected Grounds*, 100 IOWA L. REV. 1891, 1893 (2015) (citation omitted).

140. UNHCR Social Group Guidelines, *supra* note 137, ¶ 12.

141. *Id.* ¶ 13 (noting that shopkeepers or other members of a particular profession might then constitute a particular group even if “it were determined that owning a shop or participating in a certain occupation in a particular society is neither unchangeable nor a fundamental aspect of human identity”).

142. See e.g., Mark Bowden, *What Snowden and Manning Don't Understand About Secrecy*, THE ATLANTIC (Aug. 23, 2013), <http://www.theatlantic.com/politics/archive/2013/08/what-snowden-and-manning-dont-understand-about-secrecy/278973/> [https://perma.cc/VR3N-C4XD] (discussing the Snowden and Manning cases); Lauren Walker, *Glen Greenwald: Why Americans Prefer Edward Snowden to Chelsea Manning*, NEWSWEEK (July 20, 2015, 4:07 PM), <http://www.newsweek.com/glenn-greenwald-why-americans-prefer-edward-snowden-chelsea-manning-355644> [https://perma.cc/4FQ9-7ART] (contrasting Snowden with Manning); Slavoj Žižek, *Edward Snowden, Chelsea Manning and Julian Assange: Our New Heroes*, THE GUARDIAN (Sept. 3, 2013), <http://www.theguardian.com/commentisfree/2013/sep/03/snowden-manning-assange-new-heroes> [https://perma.cc/SQ5R-BVRA] (grouping Snowden together with Chelsea Manning and Julian Assange).

143. See UNHCR Social Group Guidelines, *supra* note 137, ¶ 13 (recognizing that “a particular profession might nonetheless constitute a particular social

community whistleblowers constitute a particular social group, their protected status under international refugee law hinges on whether intelligence-community whistleblowing constitutes a political act or political opinion that forms the basis for persecution.

C. Is Intelligence-Community Whistleblowing a Political Act?

Under both asylum and refugee law, the protected status of an intelligence-community whistleblower will depend on whether the requested state deems the whistleblowing a political act.

A “political offense” has important ramifications under both the Refugee Convention and asylum law more generally. Under the Refugee Convention, the UNHCR explains that, in determining whether persecution is based on political opinion, the following elements should be considered: “personality of the applicant, his political opinion, the motive behind the act, the nature of the act committed, the nature of the prosecution and its motives . . . [and] the nature of the law on which the prosecution is based.”¹⁴⁴

In asylum law, by comparison, two important models emerge in considering the political offense exception. The first is the political incidence theory, followed by the United States and the United Kingdom.¹⁴⁵ In order to qualify as a political act, it “must be part of and incidental to a political struggle.”¹⁴⁶ Intelligence-community whistleblowing would not qualify as a political act under such a theory, as “[t]here is no ongoing uprising taking place in the U.S., only disparate political rhetoric”¹⁴⁷ The other model is the proportionality theory. Under this Swiss-developed model, the whistleblowing “should be part of [or] linked with a political conflict situation [and] there should be a commensurateness between the act and the political objective of the act.”¹⁴⁸ Under this approach, the criminal nature of the act should be directly compared to its political objective. Extremely serious offenses, such as murder, “usually do not satisfy this criterion,” while “purely political” crimes, which are not common crimes and do not injure private persons, property, or interests would always satisfy such a test.¹⁴⁹

group if in the society they are recognized as a group which sets them apart”).

144. UNHCR HANDBOOK, *supra* note 30, ¶ 86.

145. Van den Wijngaert, *supra* note 26, at 746.

146. *Id.* (citing as an example the attempted murder of a British soldier in Northern Ireland by a member of the IRA, which was connected to the overall conflict in Northern Ireland).

147. Kielsingard & Gee-Kin Ip, *supra* note 70, at 64.

148. Van den Wijngaert, *supra* note 26, at 748.

149. *Id.* at 745, 748.

Intelligence-community whistleblowing would fall somewhere in between the two extremes of "serious" and "purely political" crimes.

Intelligence-community whistleblowing could potentially constitute a political offense under asylum law and possibly an act leading to persecution due to political opinion, which is protected under international refugee law.¹⁵⁰ Again, a substantial obstacle to any consensus being reached is the state-to-state variations in determining a political offense. International political pressures, economic ties and the economic or political superiority of the requesting state can all influence a state's decision to grant or deny refugee or asylee status.¹⁵¹ Because of the individualized decision-making process under both legal frameworks, a clear answer to whether intelligence-community whistleblowing constitutes a political act is elusive.

If we look to the personality, political opinion, and motive behind the act, we find some indications for why intelligence-community leakers disclosed the confidential information. Snowden explained that he was "willing to sacrifice all of that [career, salary, home, and family] because I can't in good conscience allow the US government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building."¹⁵² Chelsea Manning chose to release documents that "would 'embarrass' the country, notably the roughly 250,000 diplomatic cables revealing 'back room deals' that 'did not seem characteristic [of a country that was] so-called leader of the free world.'"¹⁵³ Thomas Drake's motivations were arguably political in nature, focused on "what he viewed as [the NSA's] mistaken decisions on costly technology programs."¹⁵⁴ The UNHCR cautions against reading the phrase "political opinion" too literally as "it may not always be possible to establish a causal link between the opinion expressed and the related measures suffered or feared by the applicant [as] [s]uch measures have only rarely been based expressly on 'opinion.'"¹⁵⁵ Nevertheless, there are some clear political motivations behind many of the intelligence-community leakers' disclosures.

150. See UNHCR HANDBOOK, *supra* note 30, ¶¶ 80–86 (outlining the circumstances under which persecution against political opinion can result in refugee status).

151. Van den Wijngaert, *supra* note 26, at 749–50.

152. Greenwald et al., *supra* note 4.

153. Reitman, *supra* note 73.

154. Shane, *supra* note 71.

155. UNHCR HANDBOOK, *supra* note 30, ¶ 81.

There is some precedent within the U.S. court system that whistleblowing against a government official may constitute "political activity." The Ninth Circuit in *Grava v. INS*,¹⁵⁶ though cautioning that whistleblowing is "not, as a matter of law, always an exercise of political opinion," when targeted against corrupt government officials, "it may constitute political activity sufficient to form the basis of persecution on account of political opinion."¹⁵⁷

There is also some indication that the prosecutions of intelligence-community leakers are overzealous and selectively enforced. A former CIA officer noted that the prosecution of John Kiriakou "seems disproportionate and more like persecution. There appears to be a vindictiveness about this."¹⁵⁸ Chelsea Manning was originally sentenced to a 35-year military prison sentence, which included lengthy stays in solitary confinement.¹⁵⁹ Facing indictment, Thomas Drake was forced from two teaching jobs before landing at an Apple computer store as he prepared his defense.¹⁶⁰ The ardent prosecution of intelligence-community leakers who release information to expose perceived government wrongdoing is all the more striking when compared to lenient treatment afforded to former four-star general David Petraeus, who gave classified information to his girlfriend and without a public interest motivation.¹⁶¹ Unlike John Kiriakou, who served prison time, Petraeus received "a slap on the wrist" by pleading guilty to a misdemeanor,

156. 205 F.3d 1177 (9th Cir. 2000).

157. *Id.* at 1181 (citing *Reyes-Guerrero v. INS*, 192 F.3d 1241, 1245 (9th Cir. 1999)).

158. Steve Coll, *The Spy Who Said Too Much: Why the Administration Targeted a C.I.A. Officer*, THE NEW YORKER (Apr. 1, 2013), <http://www.newyorker.com/magazine/2013/04/01/the-spy-who-said-too-much> [<https://perma.cc/PXZ2-UB8G>].

159. Conor Friedersdorf, *The Persecution of Chelsea Manning*, THE ATLANTIC (Aug. 13, 2015), <http://www.theatlantic.com/politics/archive/2015/08/the-ongoing-persecution-of-chelsea-manning/401195/> [<https://perma.cc/VXG5-GAKT>]. At the close of his presidency in early 2017, President Obama "commuted all but four months of the remaining prison sentence" of Manning. See Charlie Savage, *Chelsea Manning to be Released Early as Obama Commutes Sentence*, N.Y. TIMES (Jan. 17, 2017), <https://www.nytimes.com/2017/01/17/us/politics/obama-commutes-bulk-of-chelsea-mannings-sentence.html> [<https://perma.cc/6CMT-SJQJ>] (reporting that Manning is set to be freed on May 17, 2017).

160. Shane, *supra* note 71.

161. Andrew C. McCarthy, *Petraeus is Protected by a Politicized Justice Department*, NAT'L REVIEW (Mar. 5, 2015), <http://www.nationalreview.com/article/414888/petraeus-protected-politicized-justice-department-andrew-c-mccarthy> [<https://perma.cc/QGM7-7WAU>].

which carries only probation time and a fine.¹⁶² The implication of such disparate treatment is that there is “one set of rules for government insiders like Petraeus” and another—“law as a weapon—for use against Obama’s political detractors and scapegoats.”¹⁶³

III. MEASURES TO IMPROVE PROTECTION OF INTELLIGENCE-COMMUNITY WHISTLEBLOWERS

The preceding discussions reveal shortcomings in the protection afforded to intelligence-community whistleblowers at both the domestic and international levels. Alterations to the existing frameworks would allow for more transparency within governments and increased safeguards for intelligence-community employees wishing to report and correct misconduct. The alterations can be grouped into two layers of protection: (A) front-end, or domestic protections and (B) back-end, or international protections.

A. *Alterations to Domestic Law Whistleblower Protections*

Domestic whistleblower protections for intelligence-community employees should be upgraded. Nowhere is this truer than in the United States. In the minds of many employees, safeguards and incentives are missing—“CIA employees have witnessed torturing colleagues in the agency get away with their crimes[, but] [t]hey’ve watched Kiriakou go to jail after objecting to torture.”¹⁶⁴ As Snowden described, “[w]hen I was at NSA, everybody knew that for anything more serious than workplace harassment, going through the official process was a career-ender at best. It’s part of the culture”¹⁶⁵ Snowden offers a broadly

162. *Id.* (noting that, absent a plea, Petraeus “should have been charged in a multi-count indictment”).

163. *Id.*

164. Conor Friedersdorf, *Why Intelligence Whistleblowers Can’t Use Internal Channels*, THE ATLANTIC (July 28, 2014), <http://www.theatlantic.com/politics/archive/2014/07/whyintelligencewhistleblowerscantrelyoninternalchannels/375127/> [<https://perma.cc/8B7Q-VPR5>] (“Now, in the unlikely event that they weren’t previously aware of it, they’ve been put on notice that if they engage in whistleblowing through internal channels, during the course of a Senate investigation into past illegal behavior by the CIA, *even then* the protections theoretically owed them are little more than an illusion.”).

165. Spencer Ackerman & Ewen MacAskill, *Snowden Calls for Whistleblower Shield after Claims by New Pentagon Source*, THE GUARDIAN (May 22, 2016), <https://www.theguardian.com/us-news/2016/may/22/snowden-whistleblower-protections-john-crane> [<https://perma.cc/397C-6SPZ>].

described solution—"iron-clad, enforceable protections for whistleblowers and . . . a public record of success stories"¹⁶⁶—but the essential measures needed are more direct whistleblower access to Congress or an independently created body to handle complaints and an option for whistleblowers to go public if internal reporting mechanisms fail.

Domestic whistleblower legislation should first establish a body with greater independence from the executive branch to handle whistleblower complaints. This recommendation is supported by the Tshwane Principles, which suggests that "[s]tates . . . establish or identify independent bodies to receive and investigate protected disclosures . . . [which] should be institutionally and operationally independent from the security sector and other authorities from which disclosures may be made, including the executive branch."¹⁶⁷ While initial reporting within the Executive Branch may be appropriate, employees need an alternate, independent body available to them for reporting.

As it currently stands in the United States, whistleblower laws within the intelligence community allow the Inspectors General to "filter, and even block, reports to Congress from national security whistleblowers."¹⁶⁸ Employees may make reports to the Congressional intelligence committees, but must first give notice to the Director, through the Inspector General, of their intent to contact the committee and do so only "through the [Inspector General's] direction on how to contact the intelligence committees in accordance with appropriate security practices."¹⁶⁹

Daniel D'Isidoro suggests creating an Office of Special Counsel of the Intelligence Community to advocate for whistleblowers and "help them navigate the proper procedures in reporting waste, fraud, abuse, or reprisal."¹⁷⁰ Placement within the Office of the Director of National Intelligence would "allow the office to remain independent from the individual agencies' activities and pressures."¹⁷¹ However, it would still remain in the Executive Branch, and as stated by Richard Moberly, "cannot be the only option" because it would be "subject to the

166. *Id.*

167. TSHWANE PRINCIPLES, *supra* note 32, at 50.

168. Richard Moberly, *Whistleblowers and the Obama Presidency: The National Security Dilemma*, 16 EMP. RTS. & EMP. POL'Y J. 51, 123 (2012) (citations omitted).

169. Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, § 702(a)(D)(ii), 112 Stat. 2413, 2414 (codified as amended at 50 U.S.C. § 3517(d)(5)(D)(ii) (Supp. II Vol. III 2013–2015)).

170. D'Isidoro, *supra* note 44.

171. *Id.*

ultimate control of the executive branch."¹⁷² Intelligence-community whistleblowers should be able to report to a body firmly outside of the administration.

With that in mind, the most feasible solution for the intelligence-community employees in the United States is to have greater access to Congress. D'Isidoro suggests allowing an employee to "submit his complaint to the intelligence committees concurrently with submitting the complaint to the Inspector General."¹⁷³ D'Isidoro, however, reserves this measure for "emergencies."¹⁷⁴ Moberly goes further and advises that "Congress needs direct, unfiltered reports from national security whistleblowers if the executive branch does not resolve problems identified by whistleblowers."¹⁷⁵ The approach highlighted by Moberly better moves whistleblower protection forward by allowing for reporting to an independent body outside the control of the executive branch.

Greater measures should also be taken by Congress to protect the identities of whistleblowers. This is especially pressing given the news that the CIA "obtained a confidential email to Congress about alleged whistleblower retaliation related to the Senate's classified report on the agency's harsh interrogation program."¹⁷⁶ Questions about the security of communications with oversight bodies will do nothing to alleviate the "lack of faith"¹⁷⁷ in the government's official whistleblower channels.

Public disclosure should be retained as an option for intelligence-community whistleblowers if the internal mechanisms for disclosure have been exhausted, but with a high threshold to meet. Michael Scharf and Colin McLaughlin suggest allowing an employee to disclose to the media if she "(1) has a reasonably good faith belief that her allegations are accurate and that disclosure is necessary to avoid serious harm; (2) has exhausted internal procedures unless she reasonably believes that disclosure would subject her to retaliation, or that the employer would conceal or destroy the evidence if alerted; and (3) publicly identifies herself as the source of the information."¹⁷⁸

172. Moberly, *supra* note 168, at 124 (emphasis omitted).

173. D'Isidoro, *supra* note 44.

174. *Id.*

175. Moberly, *supra* note 168, at 125.

176. Marisa Taylor & Jonathan S. Landay, *After CIA Gets Secret Whistleblower Email, Congress Worries About More Spying*, McCLATCHY DC (July 25, 2014, 3:08 PM), <http://www.mcclatchydc.com/news/nationworld/national/nationalsecurity/article24771052.html> [<https://perma.cc/CB6Y-3UFT0>].

177. Ackerman & MacAskill, *supra* note 165.

178. Michael P. Scharf & Colin T. McLaughlin, *On Terrorism and Whistleblowing*, 38 CASE W. RES. J. INT'L L. 567, 579-580 (2007) (citation omitted).

Such an approach would allow for public disclosure in the event of institutional failure to address misconduct or illegality, while requiring the release of the whistleblower's name if he or she decides to go public. The ability to attach a name and face to the leaked information is critical to establishing the credibility of both the source (and their motivations) and the revelations. This is evident when comparing the approach of Edward Snowden, who publicly revealed himself, with the anonymous hacker that provided stolen CIA documents to WikiLeaks in March of 2017.¹⁷⁹ While Snowden was able to "make his case directly to the public" and start a conversation that "influenced both public policy and the law," the lingering questions surrounding the motivations and identify of the WikiLeaks source will likely prevent any similar debate over the scale and "acceptable limits of CIA spying activities."¹⁸⁰

Perhaps the biggest obstacle to formulating any intelligence-community whistleblowing policy allowing for public disclosure is determining the legally acceptable scale and scope of released information. The Tshwane Principles, for instance, would limit allowable public disclosure to the "amount of information that [is] reasonably necessary to bring to light the wrongdoing."¹⁸¹ There is no definite answer, however, as to what constitutes a "reasonably necessary" amount of information in such circumstances and how an intelligence-community whistleblower could determine that amount.

Richard Moberly suggests "limiting the disclosures to information that should not have been classified in the first place because it covered up illegality . . ."¹⁸² While it is true that, in the opinion of several experts, the United States "classifies way too much information,"¹⁸³ it

179. See Sue Halpern, *The Assange Distraction*, N.Y. REV. BOOKS: NYR DAILY (Mar. 15, 2017), <http://www.nybooks.com/daily/2017/03/15/assange-distraction-wikileaks-cia/> [<https://perma.cc/C78Z-U9UV>] (discussing the WikiLeaks "release of a portion of . . . [a] trove of classified CIA documents . . . [revealing] actual programs designed to infect, disable, or take over any number of digital devices").

180. *Id.* (arguing that "[a]s long as the public believes that WikiLeaks is working in concert with the Russians to undermine faith in American institutions, or on its own to support the Trump agenda . . . there will be no debate over the CIA's development and deployment of cyber-weapons").

181. TSHWANE PRINCIPLES, *supra* note 32, at 52.

182. Moberly, *supra* note 168, at 139.

183. Tom Blanton, Editorial, *America Classifies Way Too Much Information—and We are All Less Safe for It*, WASH. POST. (July 31, 2015), https://www.washingtonpost.com/opinions/the-united-states-is-not-safer-when-its-citizens-are-left-in-the-dark/2015/07/31/641b53fa-36e2-11e5-b673-1df005a0fb28_story.html?utm_term=.13711e6bda54 [<https://perma.cc/6DC8-7DM3>] (noting that Ronald Reagan's former executive secretary

would be a daunting task for a potential whistleblower to determine the appropriate classification or the legality of acts or policies within materials in advance of public disclosure. At a minimum, whistleblowers should remove “personal identifiers and other potentially harmful information” that is unnecessary to establishing the alleged misconduct.¹⁸⁴ Though maligned by some critics for absconding with too much information, the process employed by Edward Snowden to sort out what information to disclose may in fact be the most practical. Snowden removed himself from that determination process and instead “provided a set of documents to several journalists and asked that [they] make careful judgments about what should and should not be published based on several criteria.”¹⁸⁵ Although challenging to devise, providing some guidelines to potential intelligence-community whistleblowers on the legally acceptable scale and scope of publicly released information is essential. Such protocol would allow for the possibility of public disclosure in cases of institutional failure, but otherwise eliminate whistleblower protections for those employees that recklessly disclose excess information.

B. Alterations to International Law Whistleblower Protections

The back-end, or international approaches, would be activated in the event that intelligence-community leakers were denied due protection under domestic whistleblower law. There are two possible avenues to enhance intelligence-community whistleblower protection at the international level.

The first, more ambitious approach would focus on the creation of a new international instrument such as a treaty or convention. The proposed Snowden Treaty¹⁸⁶ is an intriguing first step put forth by advocates of intelligence community whistleblowers. The proposed International Treaty on the Right to Privacy, Protection Against Improper Surveillance and Protection of Whistleblowers, or “Snowden Treaty” as it has been described by its backers, is an alteration to the international asylum law framework that, in part, addresses the legal

for the National Security Council claimed 90 percent of “how much gets classified doesn’t deserve to be”).

184. Halpern, *supra* note 179 (indicating that the author “once came across Bill Clinton’s home phone number in a WikiLeaks file”).

185. Glenn Greenwald, *Some Facts about How NSA Stories are Reported*, THE INTERCEPT (Mar. 23, 2014), <https://theintercept.com/2014/03/23/facts-nsa-stories-reported/> [<https://perma.cc/XUL2-QTZ4>] (stating that “[p]ublication of an NSA story constitutes an editorial judgment by the media outlet that the information *should be public*”) (emphasis original).

186. The Snowden Treaty, *supra* note 28.

status of those who characterize their actions as “whistleblowing.”¹⁸⁷ The law, as officially described, would stipulate that “[w]histleblowers will not be subject to sanctions for publicly releasing information with the reasonable intent of exposing wrongdoing” and also “commits signatories to . . . guarantee the right of residence in their countries and embassies for people claiming to be persecuted as whistleblowers until the appropriate proceedings for permanent asylum have been carried out in full.”¹⁸⁸ The Snowden Treaty’s provisions for an international right to digital privacy and a global ban on mass intelligence-gathering programs may not be plausible¹⁸⁹ or even necessary.¹⁹⁰ Its proposals for increased whistleblower protection holds some promise, but may contain flaws that preclude widespread acceptance by the international community.¹⁹¹

A slightly less ambitious model would involve creating a government whistleblowing protocol, which would add a defined “government whistleblower” category to those protected under the 1951 Convention,¹⁹² which would afford protection to those fearing persecution because of actions that exposed government misconduct. Such a protocol could include a third-party adjudicator, such as the United Nations High Commissioner on Refugees, to decide the status of government whistleblowers.¹⁹³ A neutral arbiter could solve the common

187. *Id.*

188. *Id.*

189. Marko Milanovic, *The World Doesn't Need a "Snowden Treaty,"* JUST SECURITY (Oct. 21, 2015, 1:04 PM), <https://www.justsecurity.org/26984/world-doesnt-snowden-treaty/> [<https://perma.cc/ART3-Q33W>] (“It seems completely fanciful that any of the major players engaged in some type of mass surveillance (e.g., the US, the UK, Russia, or China), not to mention authoritarian regimes in many smaller states that are doing surveillance on the cheap, would ever agree to any such treaty.”).

190. *See id.* (noting that there are already widely accepted human rights conventions, such as the International Covenant on Civil and Political Rights, that protect the right to privacy).

191. *See id.* (arguing that the U.S. is particularly unlikely to ever ratify such a treaty because, in part, “even treaties that bring much more obvious benefits and little if any costs to the US, such as the Convention on the Rights of the Child or the Law of the Sea Convention,” have not been ratified).

192. Refugee Convention, *supra* note 24, at art. 1(A)(2).

193. Third-party adjudicators have frequently been utilized in settling whistleblower disputes at the national level. For instance, the use of an independent third-party to settle whistleblower disputes “is contemplated as a normal option to resolve retaliation cases in the U.S. Whistleblower Protection Act.” Tom Devine, *International Best Practices for Whistleblower Policies*, GOV'T ACCOUNTABILITY PROJECT (Nov. 25, 2015), <https://www.whistleblower.org/sites/default/files/International%20Whistleblower%20Best%20Practices%2011%2025%202015.pdf> [<https://perma.cc/Z2CY->

diplomatic and political influence that plagues the refugee determination process and prevents consistent application of refugee and asylum law.

Both of these options would face steep obstacles to gaining widespread acceptance. First, international treaties take time to implement and the United States, in particular, is hesitant to ratify any treaty that is perceived to potentially impact its national interests.¹⁹⁴ Second, even if an international agreement was created, international laws “take effect only through the actions of individual sovereign states.”¹⁹⁵ The United States would have to implement the provisions of any international covenant and “[s]tates themselves have to consent to be enforced upon”¹⁹⁶ It is unlikely that a large number of world powers would relinquish claims to prosecute leakers of classified information. Though a neutral arbiter would go far toward removing the political influences that plague the determination of refugee and asylum status, such a measure is unlikely because it would require “exclusive or appellate jurisdiction over such matters,”¹⁹⁷ which again would require a new convention or protocol to create such jurisdiction. For these reasons, a new international instrument to provide enhanced protection for intelligence-community whistleblowers is unlikely to gain much traction, at least initially.

For that reason, a second, more modest approach would be more feasible. Such an approach would work within the existing international conventions as written. Under this second scenario, the UNHCR would adjust the guidelines and handbook¹⁹⁸ to recommend clearer and

CSAN] (“Third party dispute resolution can be an expedited, less costly forum for whistleblowers. For example, labor-management arbitrations have been highly effective when the parties share costs and select the decision-maker by mutual consent through a ‘strike’ process.”).

194. *Why Won't America Ratify the UN Convention on Children's Rights?*, THE ECONOMIST (Oct. 6, 2013, 11:50 PM), <http://www.economist.com/blogs/economist-explains/2013/10/economist-explains-2> [<https://perma.cc/U3SF-RLVU>] (noting that the only countries unwilling to sign the Convention on the Rights of the Child are Somalia, South Sudan, and the United States).

195. Hannah Chang, *A 'Legally Binding' Climate Agreement: What Does it Mean? Why Does it Matter?*, STATE OF THE PLANET (Feb. 23, 2010), <http://blogs.ei.columbia.edu/2010/02/23/a-%E2%80%9Clegally-binding%E2%80%9D-climate-agreement-what-does-it-mean-why-does-it-matter/> [<https://perma.cc/VLU6-YSSE>].

196. *Id.*

197. M. Cherif Bassiouni, *Ideologically Motivated Offenses and the Political Offenses Exception in Extradition—A Proposed Juridical Standard for an Unruly Problem*, 19 DEPAUL L. REV. 217, 257 (1969).

198. UNHCR HANDBOOK, *supra* note 30.

enhanced protections for a narrowly-defined set of government whistleblowers under the 1951 Convention and the 1967 Protocol. Judicial bodies within each state would then have clearer guidance that intelligence-community whistleblowing may qualify a claimant for refugee status under the proper conditions as modeled on the Tshwane Principles.¹⁹⁹

This second approach would also consist of intensive encouragement of states to adopt domestic legislation modeled on the whistleblower guidelines of the G20 Whistleblower Study²⁰⁰ and the more narrowly tailored Tshwane Principles.²⁰¹ Lastly, the new guidelines would require that the judiciary, not the executive, determine the refugee or asylee status of applicants. Although extradition itself "is a prerogative of the government," the judiciary should, according to Paul Gully-Hart, "examine the legal requirements set forth in the treaty or in domestic legislation."²⁰² A judicial body will help to prevent political concerns from becoming the overwhelming factor in determining whether a whistleblower applicant qualifies for refugee or asylee status.

CONCLUSION: THE VALUE OF WHISTLEBLOWERS IN THE INTELLIGENCE COMMUNITY

The international community should strive to improve whistleblower protections for intelligence-community employees at both the domestic and international level. The need for secure internal reporting channels and clear guidelines on appropriate timing and methods for disclosing to the media is apparent from the heated discussion on the legacy of Edward Snowden. Because Snowden found whistleblower protections for U.S. intelligence-community employees to be insufficient, he took steps to seize and disclose classified documents publicly, without the benefit of knowing what or how much to disclose. Improving the domestic and international legal protections afforded to whistleblowers will serve the public interest while limiting mass leaks of classified state secrets.

Even Edward Snowden's detractors concede that his disclosures provided some public benefit.²⁰³ Snowden's leaks "launch[ed] an ongoing

199. TSHWANE PRINCIPLES, *supra* note 32.

200. G20 WHISTLEBLOWER STUDY, *supra* note 31.

201. TSHWANE PRINCIPLES, *supra* note 32.

202. Paul Gully-Hart, *The European Approach to Extradition*, in INTERNATIONAL CRIMINAL LAW: MULTILATERAL AND BILATERAL ENFORCEMENT MECHANISMS 343, 371 (M. Cherif Bassiouni ed., 3d. ed. 2008).

203. *See, e.g.*, Kaplan, *supra* note 97 (recognizing that "some of [Snowden's] leaks did have social and political benefits"); Editorial, *supra* note 97 (noting

national debate about the NSA's proper role in private affairs [and] [c]oncern about these activities was so great that President Obama appointed a panel of advisors to study NSA surveillance, which ultimately recommended strictly curtailing the NSA's ability to engage in warrantless data collection."²⁰⁴ Many credit Snowden with heightened public awareness of digital privacy issues²⁰⁵ and increased judicial scrutiny of government intelligence-gathering tactics.²⁰⁶ Most commentators will concede that there was a benefit to the public that came from Snowden's disclosures.

There are lingering questions, however, as to the potential cost. Many allege that Snowden released far too much information that exposed lawful, essential government programs.²⁰⁷ The House Intelligence Committee alleges that "[s]ome of Snowden's disclosures exacerbated and accelerated existing trends that diminished the [intelligence community's] capabilities to collect against legitimate foreign intelligence targets, while others resulted in the loss of intelligence streams that had saved American lives."²⁰⁸ While defenders contend that any

that "[i]t's fair to say we owe these necessary reforms [of NSA programs] to Mr. Snowden").

204. Kwoka, *supra* note 59, at 1407 (citations omitted).

205. *See, e.g.*, Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RESEARCH CTR. (Mar. 16, 2015), <http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/> [<https://perma.cc/XD6M-5JWY>] (finding that 30% of all adults "have taken at least one step to hide or shield their information from the government" and 22% of all adults say "they have changed the patterns of their own use of various technological platforms 'a great deal' or 'somewhat' since the Snowden revelations").

206. *See* Trevor Timm, *The Snowden Effect: New Privacy Wins Await After Data Transfer Ruling*, THE GUARDIAN (Oct. 8 2015), <https://www.theguardian.com/commentisfree/2015/oct/08/snowden-effect-new-privacy-wins-data-transfer-ruling> [<https://perma.cc/GR5R-37NU>] ("[O]ur digital rights is [sic] unquestionably more protected than it was when the leaks started. And with the coming court cases over the next year or two, the seismic shift will undoubtedly continue to occur").

207. *See, e.g.*, David Remnick, *Going the Distance: On and Off the Road with Barack Obama*, THE NEW YORKER (Jan. 27, 2014), <http://www.newyorker.com/magazine/2014/01/27/going-the-distance-david-remnick> [<https://perma.cc/HJF4-EF57>] (reporting that President Obama described Snowden as a "twenty-nine-year-old [who ended up having] free rein to basically dump a mountain of information, much of which is definitely legal, definitely necessary for national security, and [is] properly . . . classified[.]").

208. INTELLIGENCE COMMITTEE EXECUTIVE SUMMARY, *supra* note 3, at 1.

damage done by Snowden's disclosures is overblown²⁰⁹ or greatly outweighed by the benefit,²¹⁰ his critics charge that his acts have benefited terrorist organizations²¹¹ and cost lives and money.²¹²

Improvements to domestic and international whistleblower protection may allow societies to benefit from good-faith disclosures while avoiding the drawbacks cited by Snowden detractors. States should implement effective internal reporting channels and allow whistleblowers direct access to independent oversight bodies. Public disclosures should also be permitted to whistleblowers in the event an internal reporting channel fails, but with clearly communicated limitations on when such disclosure is appropriate and how much material may be released to the public. Upgraded reporting mechanisms and greater protections for intelligence-community whistleblowers would alert the

209. See, e.g., Eric Schmitt & Michael S. Schmidt, *Qaeda Plot Leak Has Undermined U.S. Intelligence*, N.Y. TIMES (Sept. 29, 2013), <http://www.nytimes.com/2013/09/30/us/qaeda-plot-leak-has-undermined-us-intelligence.html> [https://perma.cc/TQ9L-27GF] (“[S]ome government analysts and senior officials have made a startling finding: the impact of a leaked terrorist plot by Al Qaeda in August has caused more immediate damage to American counterterrorism efforts than the thousands of classified documents disclosed by Edward Snowden . . .”).

210. Gellman, *supra* note 3 (“I believe Snowden’s disclosures did a lot more good than harm, but I do not share the view of some of his fans that he did no damage at all.”).

211. See e.g., Michael Hirsh, ‘It’s All Back in Snowden’s Lap,’ POLITICO (Nov. 17, 2015), <http://www.politico.com/magazine/story/2015/11/paris-attack-isis-snowden-michael-morell-interview-cia-213373> [https://perma.cc/GBL6-4AAM] (quoting Michael Morrell, former acting head of the CIA, as saying “[f]irst, ISIS went to school on how we were collecting intelligence on terrorist organizations by using telecommunications technologies. And when they learned that from the Snowden disclosures, they were able to adapt to it and essentially go silent.”); Aaron Cooper, *NSA: Snowden Leaks Hurt Ability to Track Terrorists*, CNN (Feb. 23, 2015), <http://www.cnn.com/2015/02/23/politics/nsa-surveillance-north-korea/> [https://perma.cc/KZ27-CFE3] (quoting the head of the National Security Agency who claimed that the Snowden revelations “had a material impact in our ability to generate insights as to what counterterrorism, what terrorist groups around the world are doing . . .”). But see Natasha Bertrand, *Cyber Expert: Idea that Snowden Leaks Facilitated Paris Attacks is ‘A Fantastic Work of Intellectual Fiction,’* BUS. INSIDER (Nov. 20, 2015), <http://www.businessinsider.com/edwardsnowdenparisattacks201511> [https://perma.cc/E3X4-GR95] (quoting CEO of cybersecurity firm stating that “[t]here is no evidence at all that the Snowden leaks contributed or altered the kind of terrorist activity that ISIS and Al Qaeda do . . .”).

212. INTELLIGENCE COMMITTEE EXECUTIVE SUMMARY, *supra* note 3, at 2 (“[E]ven by a conservative estimate, the U.S. Government has spent hundreds of millions of dollars, and will eventually spend billions, to attempt to mitigate the damage Snowden caused.”).

government to potential abuses and waste while preventing the possible damage to national security interests that may accompany mass leaks of classified material. If states are unwilling to provide secure reporting procedures for intelligence-community whistleblowers, the international community should adjust the refugee and asylum legal frameworks to provide that missing protection to those that report government abuses and overreach under the threat of unwarranted retaliation.

Eric Connon[†]

[†] J.D. Candidate, 2017, Case Western Reserve University School of Law. Thank you to my beautiful wife Kelly who inspires me every day. I would not be here without you.