LINCOLN MEMORIAL UNIVERSITY LAW REVIEW

VOLUME 3 FALL 2015

FOREWORD:

ARTICLES:

LINCOLN MEMORIAL UNIVERSITY LAW REVIEW

VOLUME 3 FALL 2015

LINCOLN MEMORIAL UNIVERSITY LAW REVIEW

VOLUME 3 FALL 2015

FOREWORD:

ARTICLES:

LINCOLN MEMORIAL UNIVERSITY
LAW REVIEW

VOLUME 3 FALL 2015

FOREWORD
THE SNOWDEN EFFECT: THE IMPACT OF SPILLING NATIONAL SECRETS
A SYMPOSIUM SNAPSHOT

Lauren A. Mullins[*]

On Friday, January 30, 2015, the Lincoln Memorial University Duncan School of Law hosted the biennial Law Review Symposium in honor of Professor Sandra C. Ruffin.[1] Members of the Lincoln Memorial University Law Review, faculty, staff, speakers, and members of the legal community gathered in the Duncan School of Law Courtroom to discuss the implications of the national security disclosures by former government contractor Edward Snowden.

---

[*]Lauren A. Mullins, B.S., Business Administration (University of Virginia's College at Wise); M.B.A. (East Tennessee State University); Juris Doctor Candidate, May 2016 (Lincoln Memorial University Duncan School of Law); Editor-in-Chief, LMU Law Review (2015-2016).

[1] *See LMU Law Review to Present Symposium on National Security and Digital Surveillance*, DSOL NEWS/EVENTS (Dec. 31, 2014), http://law.lmunet.edu/2014/12/31/lmu-law-review-to-present-symposium-on-national-security-and-digital-surveillance-in-the-u-s/.

The Symposium speakers, who traveled to Knoxville from all over the United States, are a fascinating group of experts that offered a wide range of valuable perspectives:

Mr. James Bamford is a leading National Security Agency expert, journalist, and bestselling author of *The Shadow Factory: The Ultra-Secret NSA From 9/11 to The Eavesdropping on America*. We were fortunate to have Mr. Bamford's unique viewpoint, as he shared some of his rare personal access to Edward Snowden--three days in Moscow conducting an interview for a *Wired* magazine cover story.[2] Later in this volume, we have provided an edited transcript of Mr. Bamford's presentation.

Mr. Brett Max Kaufman is a Teaching Fellow at New York University School of Law. Formerly a national security fellow with the American Civil Liberties Union (ACLU), Mr. Kaufman brought a pro-privacy perspective with his lecture regarding the governments "collect it all" philosophy concerning intelligence information.

Professor J. Richard Broughton is an Associate Professor of Law at University of Detroit Mercy School of Law. Professor Broughton's lecture focused on the Treason Clause of the Constitution and the required mental state for its application. He argued that electronic communications that reach the enemy do not constitute treason in the absence of a specific intent to betray America. Professor Broughton graciously followed up his presentation with an article written for this volume dedicated to the Symposium.

Professor Melanie Reid is an Associate Professor of Law at LMU Duncan School of Law and former Assistant U.S. Attorney in the Southern District of Florida. Professor Reid has conducted extensive research into the constitutionality of the use of intelligence information in criminal investigations, called "parallel construction." Professor Reid deserves special recognition for her integral role in this Symposium. She developed the Symposium theme, assisted in planning for and securing a well-rounded selection of speakers, provided a presentation to accompany her recently published article *NSA and DEA Intelligence Sharing: Why It Is Legal and Why Reuters*

---

[2] *See* James Bamford, *The Most Wanted Man in the World*, WIRED, Aug. 13, 2014, http://www.wired.com/2014/08/edward-snowden/.

and the Good Wife Got It Wrong,[3] and submitted additional work tailored to this publication. Thank you, Professor Reid, for your hard work and dedication.

Mr. Chris Inglis is a former Deputy Director and 28-year veteran of the NSA holding a number of senior leadership positions in the organization. Mr. Inglis' presentation, "National Security in the Age of Cyberspace - Can Convergence, Security, Privacy, and Transparency Co-exist?" offered valuable insight from inside the government agency. His lecture covered the framework and provided real-world examples of U.S. efforts to achieve the reconciliation of the various aims embodied in the Constitution and principles that both establish and constrain the work of the federal government. An edited transcript of this presentation is published in this volume.

Ms. Elisabeth Cook is a member of the Privacy and Civil Liberties Oversight Board (PCLOB), an independent, bipartisan agency within the executive branch. Ms. Cook is a practicing attorney, formerly with the U.S. Department of Justice, and brought a wealth of knowledge on a wide range of issues involving the balancing of government transparency and the interests of national security. Her presentation focused on the legal and policy-oriented history that informs the current debate surrounding the government's need to protect classified information. Again, an edited transcript of Ms. Cook's presentation is published in this volume.

Special Agent Beth O'Brien is with the FBI and Counterintelligence Strategic Partnership. Special Agent O'Brien's presentation focused on the definition of an "insider threat" and the FBI's development of indicators and profiles of potential insider threats.

Finally, Mr. Mark Jaycox is a Legislative Analyst for the Electronic Frontier Foundation (EFF). His focused research includes issues with consumer privacy, civil liberties, surveillance law, and cybersecurity and he has completed extensive work on legislative efforts to reform the National Security Agency and update surveillance law. Mr. Jaycox

---

[3] *See* Melanie Reid, *NSA and DEA Intelligence Sharing: Why It Is Legal and Why Reuters and the Good Wife Got It Wrong*, 68 SMU L. REV. 427, 468 (2015).

presented the key items needed for reform, current proposals in Congress, and the potential outcomes.

In addition to the work and transcripts published by the Symposium participants in this volume, the following articles are included:

Professor Jason Zenor's article examines the existing legal framework and modern competing needs of national security, the defense industry, and the public interest. In examining legal protections for sources of "leaked" information, including historical examples, he suggests a new policy which favors the free flow of information and promotes whistleblowing and government transparency.

Dr. Daniel Alati's article examines the effect that Edward Snowden's national security disclosures have had thus far on the security establishments in Canada and the U.K., noting a lack of intelligence activities oversight in both countries. The article provides insight to the dearth of legislative outcomes that have occurred as a result of the U.S. leaks and suggests recommendations to prevent reoccurrence of the situation.

Many people graciously contributed to the success of this Symposium. We would like to give special thanks to: Kathy Baughman, Kate Reagan, Andrew McCree, Laura Hash, Keri Stophel, David Harmon, Robert Smith-Yanez, Union Avenue Books, Miller & Miller Court Reporters, and Dead End BBQ for their invaluable assistance and participation.

LINCOLN MEMORIAL UNIVERSITY
LAW REVIEW

VOLUME 3 FALL 2015

THE SNOWDEN AFFAIR AND THE LIMITS OF AMERICAN TREASON

J. Richard Broughton[*]

I. INTRODUCTION

"Treason" is a damning charge. Rhetorically, and legally. It was long considered the most serious of offenses, even more serious than murder. Consider, for example, that in the *Inferno*, Dante places the murderers in the Seventh Circle of Hell.[1] But the traitors occupy the Ninth and lowest Circle.[2]

[*] Associate Professor of Law, University of Detroit Mercy. I am grateful to Nadine Hammoud, Zeina Rammal, Samia Abbas, and Patrina Bergamo for their research and editorial assistance, and to the *Lincoln Memorial University Law Review* for inviting me to participate in this Symposium.

[1] *See* DANTE ALIGHIERI, INFERNO 95-99 (Mark Musa, ed. & trans., Indiana Critical Ed. 1995) (1308).

[2] *Id.* at 230-35. Here, in Canto XXXIII, Dante travels through Antenora, where he encounters famous traitors. At one point, he sees two heads frozen inside of a single hole, with the head on top gnawing on the brain of the lower head. *Id.* at 233. *See also* Paul G. Chevigny, *From Betrayal to Violence: Dante's* Inferno *and the Social Construction of Crime*, 26 L. & SOC. INQUIRY 787, 808-13 (2001) (discussing Dante's treatment of political crimes of betrayal).

Blackstone labeled treason the worst of offenses,[3] and other authorities have followed that notion.[4] But "treason" is precisely how many government officials and political leaders described Edward Snowden's disclosure of sensitive national security information.[5] Senator Dianne Feinstein, then-chair of the Senate Intelligence Committee, said Snowden committed "an act of treason."[6] House Intelligence Committee chair Mike Rogers of Michigan had similar words: "That is what we call a traitor in this country. He has traded something of value for his own personal gain that jeopardizes the national security of the United States. We call that treason."[7] Former House Speaker Newt Gingrich said on NBC's *Meet the Press* about Snowden: "[t]his was treason."[8] And Richard Clarke, former White House counter-terrorism advisor and appointed

---

[3] *See* 4 WILLIAM BLACKSTONE, COMMENTARIES *75.

[4] *See, e.g.*, Ex parte Bollman, 8 U.S. (4 Cranch) 75, 125 (1807) (opinion of Marshall, C.J.) (remarking that "there is no crime which can more excite and agitate the passions of men than treason"); Stephan v. United States, 133 F.2d 87, 90 (6th Cir. 1943) (observing that "[t]reason is the most serious offense that may be committed against the United States"); Erin Creegan, *National Security Crime,* 3 HARV. NAT'L. SEC. J. 373, 376 (2012) (calling treason "the most serious of all offenses against the nation").

[5] The Snowden affair is, of course, the subject of this symposium and the basic facts are likely well-known to most readers. For a good description of the controversy, though, see Bryan Burrough, et al., *The Snowden Saga: A Shadowland of Secrets and Light*, VANITY FAIR, *available at* http://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview (May 2014). The Snowden affair was also the subject of a recently released documentary. *See* CITIZENFOUR (Praxis Films 2014).

[6] *See* Jeremy Herb & Justin Sink, *Sen. Feinstein calls Snowden's NSA leaks an 'act of treason*,' THE HILL (June 10, 2013, 10:19 PM), http://thehill.com/policy/defense/304573-sen-feinstein-snowdens-leaks-are-treason.

[7] *See* Laura Barron-Lopez, *Rogers says Snowden committed treason*, THE HILL (Dec. 22, 2013, 11:15 AM), http://thehill.com/policy/technology/193832-rep-rogers-says-snowden-committed-treason.

[8] *See* Transcript, *Meet the Press*, NBC NEWS (June 1, 2014), *available at* http://www.nbcnews.com/meet-the-press/meet-press-transcript-june-1-2014-n121571 (remarks of Newt Gingrich).

member of President Barack Obama's expert panel on the National Security Agency, said, "What Mr. Snowden did is treason, was high crimes."[9]

The fervor to brand Edward Snowden a traitor and convict him of treason is an understandable political response to his conduct. Perhaps "treason" is simply convenient shorthand for describing serious criminal conduct involving an intentional breach of national security, not meant to describe the actual legal status of the conduct. An epithet, but not a serious legal claim.[10] But even if understandable, it nevertheless reflects potential shortcomings in the public understanding – and apparently, the understanding of our political leaders, in particular – about the law of American treason.

This, too, is understandable. Treason has been called one of the great forgotten clauses of the Constitution.[11] Despite its pedigree in our law, treason has received relatively little academic attention. J. Willard Hurst's collection of essays on treason remains the leading academic treatment of the subject,[12] but only recently – over the past decade since the

---

[9] Brian Ross & Lee Ferran, *White House NSA Panel Member: Edward Snowden's Leaks Still 'Treasonous,'* ABCNEWS (Dec. 19, 2013), http://abcnews.go.com/Blotter/white-house-nsa-panel-member-snowdens-leaks-treasonous/story?id=21277856.

[10] *See* Kristen E. Eichensehr, *Treason in the Age of Terrorism: An Explanation and Evaluation of Treason's Return in Democratic States,* 42 VAND. J. TRANSNT'L L. 1443 (2009) ("Treason is both an ancient crime and a popular epithet").

Or, perhaps, the rhetoric of treason can even fall into the category of joke-making. During the 2015 Academy Awards broadcast, host Neil Patrick Harris joked, after *Citizenfour* had received the Academy Award for Best Documentary Feature, that Snowden "could not be here tonight for some treason." *See* THR Staff, *Edward Snowden: I Laughed at Neil Patrick Harris' Treason Joke*, THE HOLLYWOOD REPORTER (Feb. 23, 2015, 12:44 PM), http://www.hollywoodreporter.com/news/edward-snowden-i-laughed-at-777125.

[11] *See* Carlton F.W. Lawson, *The Forgotten Constitutional Law of Treason and the Enemy Combatant Problem,* 154 U. PA. L. REV. 863, 865 (2006).

[12] *See* J. WILLARD HURST, THE LAW OF TREASON IN THE UNITED STATES: COLLECTED ESSAYS (1971). *See also* Willard Hurst, *Treason in the*

September 11 attacks – has the Treason Clause begun to receive greater attention from contemporary scholars.[13] Professor George Fletcher lamented many years ago that treason is no longer part of a law school course on criminal law.[14] The law of American treason thus remains underdeveloped, incomplete, and lousy with gaps. But that might actually be a good thing. A more well-developed treason law would likely require that treason be far more common. Yet treason prosecutions have been sufficiently rare in our history that relatively few opportunities have arisen for courts and lawyers to adequately answer the many questions that could arise from an accusation of, and prosecution for, treason.

Treason was a subject of some interest in the early years of the Republic – Benedict Arnold is perhaps our most famous traitor, though his betrayal at West Point occurred before the Constitution was drafted,[15] and the treason trial of Aaron Burr perhaps the most prominent one of its kind during the era, produced some early Supreme Court precedent on the meaning of American treason law.[16] Quite naturally, treason

---

United States, 58 HARV. L. REV. 226 & 395 (1945) (explaining law of treason in essays that would later form Hurst's book on treason).

[13] *See, e.g.,* Lawson, *supra* note 11; Eichensehr, *supra* note 10; Paul T. Crane, *Did the Court Kill the Treason Charge?: Reassessing* Cramer v. United States *and Its Significance*, 36 FLA. ST. U. L. REV. 635 (2009); Henry Mark Holzer, *Why Not Call It Treason?: From Korea to Afghanistan,* 29 S.U. L. REV. 181 (2002); Suzanne Kelly Babb, *Fear and Loathing in America: Application of Treason Law in Times of National Crisis and the Case of John Walker Lindh*, 54 HASTINGS L.J. 1721 (2003); George P. Fletcher, *Ambivalence About Treason*, 82 N.C. L. REV. 1611 (2004). For a collection of the scholarship that discusses treason history, see Lawson, *supra* note 11, at 866 n.7.

[14] *See* George P. Fletcher, *The Case for Treason*, 41 MD. L. REV. 193, 194 (1982).

[15] For an excellent account of General Washington's response to the Arnold affair, in a chapter appropriately entitled "Treason," see JAMES THOMAS FLEXNER, WASHINGTON: THE INDISPENSABLE MAN 141-48 (1974).

[16] *See* Ex parte Bollman, 8 U.S. (4 Cranch) 75 (1807). For an excellent account of the Burr trial, *see* R. KENT NEWMYER, THE TREASON TRIAL OF AARON BURR: LAW, POLITICS, AND THE CHARACTER WARS OF THE NEW NATION (2012).

was also a subject of debate during the Civil War period.[17] But it was not until World War II that treason prosecutions became prominent again. The 1940s saw a substantial number of treason prosecutions.[18] Then there was the infamous incident involving Jane Fonda's embrace of the North Vietnamese, which led to public branding of her as a traitor and the unflattering nickname of "Hanoi Jane."[19] Finally, it was in the post-September 11 world and the American effort to grapple with the problem of its own citizens joining forces with international terrorists that treason reemerged as a more serious prosecutorial option for the federal government.

John Walker Lindh offers an example. Though he traveled to the Middle East to study Arabic, Lindh later trained with a terrorist group and crossed from Pakistan into Afghanistan and joined a group of fighters that were funded by Osama bin Laden.[20] The group sent him to fight with the Taliban against the Northern Alliance.[21] He eventually surrendered to the Northern Alliance, and was recaptured after being temporarily freed during an armed attack by Taliban detainees upon a CIA operative who had been interviewing Lindh.[22] Lindh was indicted and eventually pleaded guilty to charges of providing services to the Taliban and carrying an explosive device during commission of a felony.[23] He is serving a twenty-year sentence in federal prison today. And Yasser Esam Hamdi, a native of Louisiana, rather than being prosecuted in a civilian American court was instead detained on a Naval brig and never charged by the

---

[17] *See* JONATHAN W. WHITE, ABRAHAM LINCOLN AND TREASON IN THE CIVIL WAR (2011).

[18] *See* Crane, *supra* note 13, at 638-39, 677-78.

[19] *See* Holzer, *supra* note 13, at 210-13. Unlike Holzer, Fletcher does not see Fonda's conduct as treasonous. *See* Fletcher, *supra* note 14, at 200.

[20] *See* Indictment, United States v. Lindh, No. 02-37a (E.D. Va. Feb. 5, 2002).

[21] *Id.*

[22] *Id.*

[23] *Id.* Some have argued that the Government should have charged Lindh with treason. *See, e.g.*, Holzer, *supra* note 13, at 220-21; Douglas W. Kmiec, *Try Lindh for Treason, It's Not Too Late*, National Review Online, (posted Feb. 12, 2002).

Department of Justice with a crime.[24] His case eventually went to the Supreme Court, which held that the President enjoyed the power to detain Hamdi as an enemy combatant, but that he was entitled to some process to challenge his detention.[25] But it was Justice Scalia's dissent in *Hamdi* that invoked treason. Scalia, joined by Justice Stevens, argued that where an American citizen is captured fighting for the enemy, the government has two options: suspend the writ of habeas corpus, or try him for treason or some other crime.[26] In Hamdi's case, the Government did neither.

Finally, in 2006, the Government obtained its first treason indictment since World War II, when it charged Adam Gadahn with treason after Gadahn appeared in al Qaeda videos.[27] In them, he appeared with bin Laden and Ayman al-Zawahiri, praised the September 11 attacks and encouraged al Qaeda to use its capability to attack the United States again.[28] Gadahn was never captured and tried; rather, he was killed in January 2015 during a counterterrorism operation.[29]

Perhaps treason has fallen out of favor with federal prosecutors because of the enhanced evidentiary requirements that necessarily come with a treason prosecution. Perhaps it is because other statutes exist that reach the same types of conduct without the burdens that come with the definition of treason – material support for terrorism, rebellion or insurrection, seditious conspiracy, advocating overthrow of the government, and recruiting others for service in armed hostility against the United States all come to mind. Perhaps it

---

[24] Hamdi v. Rumsfeld, 542 U.S. 507 (2004).

[25] *Id.* at 524, 533.

[26] *Id.* at 554 (Scalia, J., dissenting).

[27] *See* First Superseding Indictment, United States v. Gadahn, SA CR 05-254 (C.D. Cal. Oct. 11, 2006).

[28] *Id.*

[29] *See* Greg Botelho & Ralph Ellis, *Adam Gadahn, American mouthpiece for al Qaeda, killed*, CNN.COM, http://www.cnn.com/2015/04/23/world/adam-gadahn-al-qaeda/ (posted Apr. 23, 2015). For a brief discussion of the Gadahn case, and a suggestion that the Government used the wrong theory of treason with respect to Gadahn's conduct, see Kristen Eichensehr, *Treason's Return*, 116 YALE L.J. POCKET PART 229 (2007). Crane's article on *Cramer* also discusses the Gadahn case. *See* Crane, *supra* note 13, at 636.

is some combination of these.[30] Perhaps, as George Fletcher has argued, the decline of treason has less to do with proof of the elements and more to do with changing attitudes toward crime and criminal law.[31] The feudal bases of treason are simply inconsistent with the liberal version of the criminal law that prevails today, a criminal law that prefers "systematic and scientific control of violence" to the symbolism of ancient treason law.[32] But perhaps, in some cases at least, the trouble is not with proving the traitor's actions but, rather, his intent. Intention, Hurst observed, is "at the heart" of treason.[33] How does American treason law apply to one who communicates information that can be, and in fact is, both helpful and readily available to the enemy, or commits an overt act that in fact assists the enemy, but who does not simultaneously specifically intend to betray the United States? American criminal law has long valued the imposition of mens rea, both as a check on the power of the state and as a method for measuring culpability.[34] And a charge as serious as treason most surely requires proof of some heightened state of moral culpability at the time of the alleged overt act.

The Snowden case therefore presents a distinctly modern wrinkle in the application of treason law, one that is implicated by the popular cry of "treason" against Snowden. It raises the problem that one may aid and comfort the enemy without actually intending to do so as a way of betraying America. Can we (should we) still call that treason? That is the specific problem I want to explore. To do that, I will describe the American law of treason by giving special attention to the provision for adhering to the enemy, giving them aid and comfort (what I will call Adherence Treason, to distinguish it from Levying War Treason) and the mental state that American treason law requires for a conviction on this ground. My project, then, is to explain why it is the mens rea element of treason law that complicates that law's application to Snowden's case, and indeed in any case in which an

---

[30] *See* Crane, *supra* note 13, at 680-93.
[31] *See* Fletcher, *supra* note 14, at 1628.
[32] *Id.*
[33] HURST, *supra* note 12, at 15.
[34] *See* JOSHUA DRESSLER, UNDERSTANDING CRIMINAL LAW § 10.01, at 117 (6th ed. 2012).

American has aided the enemy through an electronic communication.

II. AMERICAN TREASON LAW AND THE EMERGENCE OF TREASON MENS REA

Treason is the only crime that the federal Constitution explicitly defines. "Treason against the United States," the text says,

> shall consist only in levying war against them, or in adhering to their enemies, giving them aid and comfort. No person shall be convicted of treason unless on the testimony of two witnesses to the same overt act, or on confession in open court. The Congress shall have the power to declare the punishment of treason, but no attainder of treason shall work corruption of blood, or forfeiture except during the life of the person attained.[35]

Congress has also codified treason as a federal crime, at section 2381 of Title 18. But because the crime of treason is constitutionalized, Congress cannot alter or modify the definition of treason by ordinary legislation. So Section 2381 provides that: "Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason and shall suffer death, or shall be imprisoned not less than five years and fined under this title not less than $10,000; and shall be incapable of holding any office under the United States."[36] As treason is punishable by death, Congress has enacted a set of procedures for capital treason prosecutions that is distinct from the procedures employed in typical capital murder prosecutions at the federal level.[37]

---

[35] U.S. CONST. art. III, §3.

[36] 18 U.S.C. §2381 (2012).

[37] In a capital treason prosecution, the list of statutory aggravating factors is shorter than for capital homicide prosecutions, 18 U.S.C. § 3591(a) (2012), and the Government need not prove the specific

Notice the word "only" in the constitutional text: there are *only* two ways to commit treason – by levying war against the United States, or by giving aid and comfort to the enemy (which is how one *adheres* to the enemy). This is a product of design. The Framers of the Constitution explicitly desired a limited treason in America.[38] The crime was meant to be narrow, more narrow even, than its chief English antecedent. The Statute of 25 Edward III, enacted in 1351, created seven basic categories of treason for purposes of English law: compassing or imagining the death of the king, or queen, or their eldest son and heir; violating the wife of the king or the wife of the king's eldest son; levying war against the king in his realm; adhering to the king's enemies in his realm, giving them aid and comfort in the realm or elsewhere; counterfeiting; killing the chancellor, the treasurer, or the king's justices; murder of a master by a servant, a husband by a wife, or a prelate by a cleric (this was called "petty treason"; the other categories were "high treason").[39] This statute did away with the common law of treason in England and was greatly admired not only by English authorities,[40] but also by American colonists and the founders, who drew upon its language in crafting colonial treason law and the constitutional definition.[41] With the development of treason law in America in the aftermath of the Revolution, however, it became clear that certain forms of English treason would not apply here.[42] Of course, many of the categories of English treason were predicated upon acts taken against the monarchy, and America would not be a monarchy. Americans could have adopted some of these provisions and

---

statutory mental state factors related to death that are required in a capital homicide prosecution. *Compare* 18 U.S.C. §3591(a)(1) *with* 18 U.S.C. §3591(a)(2)(A-D).

[38] *See* HURST, *supra* note 12, at 130.

[39] Statute of Treasons, 25 Edw. III, ch. 2 (1351).

[40] *See* EDWARD COKE, THE THIRD PART OF THE INSTITUTES OF THE LAWS OF ENGLAND 2 (London, 5th ed. 1671).

[41] *See* HURST, *supra* note 12, at 130-40. Curiously, as Hurst explains, the original draft of the Constitution did not contain a treason provision. *Id.* at 129. The Committee of Detail created and inserted the Treason Clause into the Constitution. *Id.* The Convention then fully discussed the new language on August 20, 1787. *Id.* at 130.

[42] *Id.* at 106, 126.

simply made them acts against elected political leaders, but many of these notions were never considered.

Moreover, the leading founder on treason, Pennsylvania's James Wilson (who served on the Committee of Detail that drafted the Treason Clause), argued that 25 Edward III was the chief basis for our treason law and that American treason should be interpreted in light of that statute.[43] Other leading authorities agreed.[44] Wilson remarked that the charge of treason was a dangerous charge, so it was important to limit the Government's power to bring it, thus further explaining the narrowness of American treason under the Constitution.[45] And Chief Justice Marshall, in narrowly construing the text of the Treason Clause in *Ex Parte Bollman*, said that "[a]s there is no crime which can more excite and agitate the passions of men than treason, no charge demands more from the tribunal before which it is made a deliberate and temperate inquiry."[46] The Constitution offers a limited notion of treason, Marshall wrote, "[t]o prevent the possibility of those calamities which result from the extension of treason to offenses of minor importance."[47] Constructive treasons, in particular, were viewed by the founding generation as a threat to political liberty, so the evolution of American treason law was careful to avoid these dangers.[48] Hamilton, in responding

---

[43] *See* HURST, *supra* note 12, at 135.

[44] *Id.* at 130-31.

[45] JAMES WILSON, 3 COLLECTED WORKS OF JAMES WILSON 1149-50 (Mark David Hall & Kermit Hall, ed. 2007), *available at* http://oll.libertyfund.org/titles/wilson-collected-works-of-james-wilson-vol-2. Wilson says, referring to Montesquieu's observations, that treason "is indeterminate," which "along is sufficient to make any government degenerate into arbitrary power." *Id.* at 1149. He continues that in both monarchies and republics, treason law "furnishes an opportunity to unprincipled courtiers, and to demagogues equally unprincipled, to harass the independent citizen, and the faithful subject, by treasons, and by prosecutions for treasons, constructive, capricious, and oppressive." *Id.*

[46] Ex Parte Bollman, 8 U.S. (4 Cranch) 75, 125 (1807).

[47] *Id.* at 125-26.

[48] *See* Cramer v. United States, 325 U.S. 1 (1945) (discussing the negative view of constructive treasons among the founding generation). *See also* Stephan v. United States, 133 F.2d 87, 90 (6th Cir.

to the complaint that the original Constitution contained no bill of rights, even included the Treason Clause among those constitutional provisions (beyond the structural ones) that offered protections to the individual against government action.[49]

So the first principle we can derive from the definition of American treason – and one that would militate against a treason charge for someone like Snowden – is that it is deliberately narrow and does not embrace constructive or questionable treasons.

The other thing worth noticing about the text's definition of the crime is that it does not include an explicit mens rea term. Or does it? In some ways, this should be unsurprising. The English Treasons Statute, 25 Edward III, did not contain familiar common law mens rea terminology. And still, by the time of the framing, mens rea was well-known to the English courts, the English common law, and to colonial criminal law.[50] Blackstone highlighted the state of mind that makes for treason noted in light of the English law, stating that "a bare intent to commit treason is many times actual treason: as imagining the death of the king, or conspiring to take away his crown."[51] Early treason case law referred to treasonous intention.[52] And Justice Story spoke of "intention" and "treasonable purpose" while adjudicating a treason case in Rhode Island[53] (though he offered his statement of the law with respect to levying war, rather than

---

1943) (stating "[t]he Constitution has left no room for constructive treason").

[49] *See* THE FEDERALIST NO. 84, at 511 (Alexander Hamilton) (Clinton Rossiter, ed., 1961).

[50] *See* Paul H. Robinson, *A Brief History of Distinctions in Criminal Culpability*, 31 HASTINGS L.J. 815 (1980). *See also* WAYNE R. LAFAVE, CRIMINAL LAW §5.1(a), at 253 (5th ed. 2010) (noting that since about 1600, common law judges defined crimes to contain some bad state of mind, and setting forth conventional common law mens rea terms).

[51] 4 WILLIAM BLACKSTONE, COMMENTARIES *35.

[52] *See* United States v. Hoxie, 26 F. Cas. 397, 399 (C.C.D. Vt. 1808) (No 15,407); United States v. Pryor, 27 F. Cas. 628, 630 (C.C.D. Pa. 1814) (No. 16,096).

[53] *See* Charge to the Grand Jury – Treason, 30 F. Cas. 1046, 1047 (C.C. D. R.I. 1842) (No. 18.275).

adhering to the enemy, and defined the treasonable purpose broadly).[54] But none of these early authorities meaningfully explained the precise culpable mental state that the government must prove to establish treason.

Despite the lack of clarity in the constitutional or statutory text as to the precise mens rea required for treason, it is generally agreed today that treason requires a specific intent to betray the United States. Perhaps the most important treason case of the modern Supreme Court is *Cramer v. United States*,[55] decided in 1945, and it is here where we first encounter the modern Court's discussion of treason mens rea.

In 1942, German submarines arrived at the coasts of Long Island and Florida.[56] Four men exited each sub and buried their Nazi uniforms and then dressed as civilians.[57] They had trained at a sabotage school in Germany and were supposed to destroy American war infrastructure.[58] Although all of the men had lived in the United States, all but one were German citizens. [59] They were eventually arrested and tried in military tribunals, which the Supreme Court validated in *Ex parte Quirin*.[60] Cramer was born in Germany but was naturalized in the United States in 1936.[61] He befriended Warner Thiel, who would become one of the aforementioned

---

[54] *See* Lawson, *supra* note 11, at 911 (explaining Story's view). Lawson also helpfully notes that an early Nevada statute, defining "levying war" treason for state law purposes, contained an explicit mens rea element: "when persons arise in insurrection with the intent to prevent, in general, by force and intimidation, the execution of statute in this state, or to force its repeal." *Id.* at 912 (citing NEV. REV. STAT. ANN. §196.020 (LexisNexis 2011)). The statute includes, but does not define, adhering to the enemies of Nevada, giving them aid and comfort.

[55] 325 U.S. 1 (1945). Crane's article offers a valuable history of the case, as well as of the Justice's decision-making. *See generally* Crane, *supra* note 13.

[56] *See* Ex parte Quirin, 317 U.S. 1, 21 (1942).

[57] *Id*.

[58] *Id*.

[59] *Id*.

[60] *Id.* at 48. The Court held that Herbert Hans Haupt, one of the saboteurs, could be tried by military commission, rather than by civilian court for treason, even though he may have been an American citizen. *Id.* at 38.

[61] *Cramer*, 325 U.S. at 3-4.

Nazi saboteurs.[62] They were roommates and even engaged in a joint business venture.[63] Responding to an anonymous note, Cramer went to Grand Central Station and met Thiel for drinks.[64] They then met two more times and Thiel gave Cramer a money belt with $3,600 in it.[65] Cramer kept a portion, set aside a portion in case Thiel needed it, and then put the rest in a safe deposit box.[66] The FBI observed two of the meetings and arrested Cramer.[67] Cramer was tried for treason, but said he lacked any treasonous intent and that his overt acts did not, on their face, manifest treason.[68]

The Supreme Court held for *Cramer*. In the course of doing so, the Court held that Congress could criminalize treasonous conduct under other statutory crimes without all of the procedural safeguards and limitations that attend treason itself.[69] The Court also recognized that the overt act need not manifest treasonous intent.[70] However, the overt act must actually give aid and comfort to the enemy.[71] Cramer's meetings with Thiel did not satisfy this standard.[72] With respect to the mental element of the crime, the Court grounded treason mens rea in the textual requirement of "adherence" to the enemy. "A citizen may favor the enemy and harbor sympathies or convictions disloyal to this country's policy or interest, but so long as he commits no act of aid or comfort to the enemy, there is no treason," Justice Jackson's opinion declared.[73]

---

[62] *Id.* at 4.
[63] *Id.* at 3-4.
[64] *Id.* at 5.
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.* at 31. *See also* Crane, *supra* note 13, at 642 (describing Cramer's claims before the Court). According to Crane, Cramer claimed he did not possess treasonous intent because he was unaware of Thiel's sabotage plans and met with Thiel simply as a friend. *Id.*
[69] *Cramer*, 325 U.S. at 45.
[70] *Id.*
[71] *Id.* at 39-40.
[72] *Id.*
[73] *Id.* at 29.

> On the other hand, a citizen may take actions, which do aid and comfort the enemy – making a speech critical of the government or opposing its measures, profiteering, striking in defense plants or essential work, and the hundred other things which impair our cohesion and diminish our strength – but if there is no adherence to the enemy in this, if there is no intent to betray, there is no treason.[74]

The opinion elaborated upon treason mens rea by stating that "[q]uestions of intent in a treason case are even more complicated than in most criminal cases because of the peculiarity of the two different elements which together make the offense."[75] Treasonous intent cannot be shown through overt acts that are negligent or undesigned.[76] Rather, "to make treason the defendant must not only intend the act, but he must intend to betray his country by means of the act."[77] Treasonous intent can be inferred from conduct (including the relevant overt act itself), and one is deemed to intend the natural consequences of his actions.[78] Here, however, the overt acts that the Government alleged were relatively trivial and did not themselves demonstrate treasonous intent.[79] The Court also proved unwilling to find treason merely from an alleged treasonous intent in meeting with Thiel and another man named Edward Kerling (leader of the saboteurs), concluding that those acts did not actually have the effect of giving aid and comfort to the enemy.[80] To conclude otherwise would "carry us back to constructive treasons."[81]

The first time that the Court ever affirmed a treason conviction was in *Haupt v. United States*.[82] There, a father of one of the Nazi saboteurs and an American citizen – Hans

---

[74] *Id.*
[75] *Id.* at 31.
[76] *Id.*
[77] *Id.*
[78] *Id.* at 31-32.
[79] *Id.* at 39-40.
[80] *Id.* at 40.
[81] *Id.*
[82] 330 U.S. 631 (1947).

Max Haupt – was convicted of treason after giving his son (Herbert Hans Haupt) shelter, finding him a job, and giving him a car, all while knowing that his son was on the sabotage mission.[83] Relying on the understanding of the overt act from *Cramer*, the Court held that these acts by Haupt were sufficient to actually give aid and comfort to the enemy.[84] But the Court was also satisfied that Haupt possessed the requisite treasonous intent.[85] Because Haupt knew of his son's role, his aid to his son was not mere fatherly care. It was done with the purpose of assisting his son in executing the German sabotage effort, not just of aiding his son as a son.[86]

Following the lessons of *Haupt* and *Cramer* in the world of treason mens rea is *Kawakita v. United States*,[87] another case arising out of actions amid World War II. There, Tomoya Kawakita was a dual Japanese-American citizen who traveled to Japan to study at Meiji University.[88] He renewed his passport in 1941 and took the oath of allegiance to America.[89] After school, and after registering with a family census registry in Japan (the Koseki), he later accepted a job with Oeyama Nickel Industry Company, that provided metals for the Japanese war effort.[90] That company also employed American prisoners of war, and Kawakita was originally hired as an interpreter for communications between the Japanese and the American POWs.[91] Kawakita's treason charge was based on several different alleged overt acts, all of which involved severe maltreatment of the American POWs who

---

[83] *Id.* at 632-33. The son Herbert, of course, was among those convicted in *Quirin*.
[84] *Id.* at 636.
[85] *Id.* at 641-42.
[86] *Id.*
[87] 343 U.S. 717 (1952).
[88] *Id.* at 720. The threshold issue before the Supreme Court was whether Kawakita had renounced his American citizenship, thus exempting him from American treason law (because, if true, he would no longer owe allegiance to the United States). *Id.* at 720-36. The Court rejected his claim, finding that he retained his dual citizenship. *Id.* at 736. This issue was the basis for Chief Justice Vinson's dissent. *Id.* at 745-46 (Vinson, C.J., dissenting).
[89] *Id.* at 720.
[90] *Id.*
[91] *Id.* at 720-21.

worked at the company.[92] He was tried for, and convicted of, treason when, after returning to the United States in 1946, a former American POW at the nickel company recognized Kawakita.[93]

In affirming the conviction, Justice Douglas's opinion for the Court explained that treason requires both giving aid and comfort to the enemy (the physical act required) and treasonous intent (the mens rea). "One may think disloyal thoughts and have his heart on the side of the enemy. Yet if he commits no act giving aid and comfort to the enemy, he is not guilty of treason," Douglas wrote.[94] "He may on the other hand commit acts which do give aid and comfort to the enemy and yet not be guilty of treason, as for example when he acts impulsively with no intent to betray."[95] The Court then explained that although the constitutional requirement of two witnesses applies to the physical overt act, the requirement does not extend to the mens rea.[96] Rather, the Court said, the treasonous intent is inferred from conduct, from the overt acts, from the defendant's statements about the war, and, as here, from the defendant's professions of loyalty to the enemy nation.[97]

Against this judicial backdrop, one can see why a treason prosecution against Edward Snowden would be a daunting task. Snowden himself has publicly discussed the controversy (in Moscow, he has apparently built his own studio for conducting interviews).[98] He has stated publicly

---

[92] *Id.* at 737-39.
[93] *Id.* at 722.
[94] *Id.* at 736.
[95] *Id.*
[96] *Id.*
[97] *Id.* at 742-43.
[98] *See* Katrina vanden Heuvel & Stephen F. Cohen, *Edward Snowden: A 'Nation' Interview*, THE NATION (Oct. 28, 2014), http://www.thenation.com/article/186129/snowden-exile-exclusive-interview#; James Bamford, *The Most Wanted Man in the World*, WIRED, Aug. 13, 2014, http://www.wired.com/2014/08/edward-snowden/; Alan Rusbridger & Ewen MacAskill, *Edward Snowden interview – the edited transcript,* THE GUARDIAN (July 18, 2014), http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript; Burrough, et al.,

that his desire – his intent, if you will – was to alert the public to the scope of the American surveillance regime and to spur changes that would mitigate the surveillance state and hold public officials accountable.[99] At no point does he state that it was his intention to aid the enemy in a war against America or to assist in planning an attack on the United States. Now, of course, one might imagine that he would *never* publicly say that, even if it were true. He is fully aware that he faces criminal charges and his statements seem naturally self-serving. But the point is that in the absence of such a confession, the prosecution would have to obtain other objective evidence of a desire to do just that, to adhere to the enemy by intending to betray the United States. At least on the existing publicly-available evidence, that would be difficult indeed. One need not agree with his actions in order to concede that there is insufficient evidence of his adherence to the enemy.

Now, this is not to say that such evidence is impossible to discover. In *Kawakita*, for example, the defendant made repeated statements about his desire to see America harmed. The statements included "It looks like MacArthur took a run-out powder on you boys;" "The Japanese were a little superior to your American soldiers;" You Americans don't have no chance. We will win the war;" "Well, you guys needn't be interested in when the war will be over because you won't go back; you will stay here and work. I will go back to the States because I am an American citizen;" "We will kill all you prisoners right here anyway, whether you win the war or lose it. You will never get back to the States;" "I will be glad when all of the Americans is dead, and then I can go home and live happy."[100] If the Government could find such statements from Snowden – for example, that he hoped his disclosures would assist the enemy in perpetrating an attack, or that an attack on

---

supra note 3. *See also* Inside the Mind of Edward Snowden: Interview with Brian Williams, NBC NEWS, *available at* http://www.nbcnews.com/feature/edward-snowden-interview (aired May 29, 2014) (appearing on television for interview with NBC anchor Brian Williams).

[99] James Bamford, *The Most Wanted Man in the World*, WIRED, Aug. 13, 2014, http://www.wired.com/2014/08/edward-snowden/.

[100] *Kawakita*, 343 U.S. at 743.

American interests, citizens, or military capabilities would teach us a valuable lesson about our national intelligence policies – then the case for treason would be measurably stronger. But if Snowden's desire was merely to alert the public to policies with which he disagreed, then, however misguided his tactics, that state of mind is an unlikely candidate for treasonous intent.[101]

The "intent" of treason, then, seems a lot like motive. Indeed it is. One may object that intent and motive are not the same. And they are not. But "intent," as such, is a difficult word to understand in isolation. The criminal law, particularly in the world of specific intent crimes, often makes motive relevant to proof of the offense.[102] For example, one of the ways in which we distinguish a traditional specific-intent crime is to say that it is one that requires some special motivation for its commission (such as when we require "the intent to steal" or the "intent to kill").[103] Moreover, other crimes, such as hate crimes,[104] are defined by the special motive that attends their commission. Though the relevant act (e.g., causing bodily harm) may be performed intentionally or knowingly, it is a hate crime only when the act is performed with a particular bias motivation (e.g., because of the victim's actual or perceived race or religion).[105] Treason is substantially similar. The Government must prove that the underlying overt act of providing aid and comfort to the enemy was done with a purpose to betray the United States and that purpose will often merge with the particular motive to see harm befall the country. Still, courts have been reluctant to make too much of this overlap. In two of the World War II treason prosecutions involving Americans who worked as radio broadcasters for the Germans – *Chandler v. United States*[106] and *Best v. United States*[107] – the defendants argued

---

[101] This conclusion makes comments like those of Speaker Gingrich on *Meet the Press* all the more perplexing. Gingrich said that Snowden "may be a patriotic traitor. He may think, in his own mind, he did the right thing. This was treason." *See* Meet the Press Transcript, *supra* note 8.

[102] *See* DRESSLER, *supra* note 34, §10.04[A][2], at 123.

[103] *Id.* at 138.

[104] *See* 18 U.S.C. § 249 (2012).

[105] *Id.*

[106] 171 F.2d 921 (1st Cir. 1948).

that even though they intended to aid the German war effort and to create disunity and harm to American morale during the war, they had the special motive of rendering such aid because, they argued, it would be better for Americans by halting the pursuit of world domination by Jewish Communism.[108] In each case, the First Circuit rejected the claim that this motive negated their intent to betray, because each defendant had the purpose of aiding the enemy.[109] Contrary to the First Circuit's analysis,[110] though, motive was actually *not* irrelevant in these cases. The defendants *had* a treasonous motive – in addition to their purpose to render aid to Germany, they also were motivated directly by a desire to see Germany prevail in the war (which would necessarily mean an American defeat).[111] It was simply mixed with yet another, somewhat more attenuated, motive. In this sense, the mixed motives appear similar to the mixed motives of Hans Max Haupt.[112] It is difficult to imagine a case in which the actor has the *purpose* of aiding the enemy in harming or defeating the United States, and yet he is acting solely with a motive that does not involve such harm or defeat but rather

---

[107] 184 F.2d 131 (1st Cir. 1950).

[108] *See Chandler*, 171 F.2d at 925. In each case, the defendant had served as a broadcaster for a German radio station. *See id.* at 926; *Best,* 184 F.2d at 134. The purpose of the broadcasts was to engage in "psychological warfare" to support the German war effort. *Chandler,* 171 F.2d at 926. The radio broadcasts were directed by the German Propaganda Ministry. *Id.* Broadcasting for the enemy was a popular basis for a treason charge during this period. *See also* Gillars v. United States, 182 F.2d 962 (D.C. Cir. 1950) (involving broadcasting for the Germans); D'Aquino v. United States, 192 F.2d 338 (9th Cir. 1951) (involving broadcasting for the Japanese).

[109] *Chandler*, 171 F.2d at 942-45; *Best,* 184 F.2d at 137-38.

[110] *Chandler,* 171 F.2d at 944 (holding that one who "trafficks with enemy agents" and gives them aid and comfort "is guilty of treason, whatever his motive.").

[111] *Id.* at 944.

[112] *See* HURST, *supra* note 12, at 245 (arguing that *Haupt* holds that as long as one of the mixed motives is to betray the United States, the existence of a more pure motive is irrelevant). Hurst argues that *Chandler* and *Best* are related, but distinct, on the question of motive. *Id.* As indicated here, I find them more similar on this point than does Hurst.

would benefit America. The specific "intent" of treason, and the bad *motive* that distinguishes it, simply converge.

One may argue (the Government certainly did in *Cramer*)[113] that the Court's approach makes treason too difficult to prove. Treason, one may contend, could be an especially powerful prosecutorial tool in times of national emergency or, as today, when grave dangers can be posed to national security as a result of advances in technology that make communicating with the enemy so easy. The Court's response to this, and one that arguably would fit the view of the Constitution's Framers, was simple: treason is supposed to be hard to prove.[114] Its difficulty helps to protect against politically vindictive prosecutions or the punishment of those who merely think disloyal thoughts. Yet, as *Haupt* and *Kawakita* certainly show us, the task is not impossible. Specific intent is not, and has never been, an insurmountable barrier to conviction, even in treason law.[115] And in light of the ways in which electronic or digital communication can ease the provision of aid and comfort to America's enemies, Adherence Treason could arguably form a larger share of federal prosecutorial energy and resources in the coming years. After all, as the many stories of Americans who have lately sought to join forces with the Islamic State in Iraq and Syria (ISIS) demonstrate, many of those who have joined the cause of America's enemies have not been shy about expressing their adherence to those that would harm us.[116]

---

[113] *Cramer*, 325 U.S. at 45.

[114] *See supra* text accompanying notes 42-44.

[115] *See Haupt*, 330 U.S. at 641-42; *Kawakita*, 343 U.S. at 743.

[116] *See, e.g.*, Ed Payne, *More Americans volunteering to help ISIS*, CNN (posted Mar. 5, 2015, 4:55 PM), available at http://www.cnn.com/2015/03/05/us/isis-us-arrests/; *see also* Gadahn Indictment, *supra* note 27.

Incidentally, whether ISIS (or, ISIL) currently constitutes an "enemy" of the United States for purposes of treason law is perhaps an open question, particularly in the absence of a specific authorization for the use of force against that group. I leave that question for another time, and assume for the purposes of this article that ISIS could be an enemy for treason purposes (and I currently believe that is the better understanding of the issue). Eichensehr offers an excellent discussion of this issue in her piece, though ISIS did not emerge until after her piece was published, and so her focus

III. ADHERENCE TREASON AS A SPECIES OF COMPLICITY?

This "intent to betray" doctrine that I have discussed is now well-established. It has been repeated in the Supreme Court, repeated by other courts, and repeated in the literature on treason. More than anything, as I have explained, that is the principle that would foreclose treason liability for Edward Snowden. And yet, established though it is, the derivation of this notion remains unclear.

I asked earlier whether the text really does contain a mens rea element. It does not, after all, do so in the conventional way. There is no familiar, common law mens rea term (no "intentionally," or "willfully," for example), and especially no language common to the notion of specific intent (such as "with the intent to . . ."). But it is nearly impossible to imagine treason as a strict liability offense and it has never been understood that way in American law. The federal criminal law of mens rea has been inconsistent about its rationales for requiring mens rea where it is not codified in the statute.[117] There is no federal common law of crimes (all federal criminal law is statutory) and federal courts have been reluctant at times to force common law notions onto congressional legislation or federal criminal law doctrine.[118] Still, federal criminal law has developed the following principle: absent evidence that Congress intended something to the contrary, and unless the offense falls into a category of public welfare regulations that would permit strict liability, courts presume Congress meant for some mens rea to apply to federal crimes.[119] This is particularly true, the Court has said,

---

is on other non-state actors. *See* Eichensehr, *supra* note 10, at 1491-98, 1505.

[117] *Compare* Morissette v. United States, 342 U.S. 246 (1952) *with* United States v. Dotterweich, 320 U.S. 277 (1943); United States v. Balint, 258 U.S. 250 (1922). *See also* United States v. X-Citement Video, Inc., 513 U.S. 64 (1994) (describing the Court's approach to mens rea in federal cases where mens rea terms are missing from statute).

[118] *See* United States v. Hudson & Goodwin, 11 U.S. 32 (1812).

[119] *See Morissette*, 342 U.S. at 252-53. *See also* Staples v. United States, 511 U.S. 600, 605 (1994) (stating the preference for requiring mens rea, and that congress must clearly intend for a criminal statute to dispense with mens rea).

where the crime is one against the state (like treason), the person, property, or public morals.[120] So even in the absence of an explicit mens rea element, our natural inclination would be to interpret the Treason Clause to impose one. There is no sound reason, then, to doubt *Cramer's* explication (or that of earlier cases from lower courts) of the law of treason as requiring a culpable mental state.

Cramer, though, understands the word "adhering" as necessarily embracing the mental element of *intentional* betrayal. "Adherence to the enemy," Justice Jackson said, is the "disloyal state of mind" that the Government must prove.[121] This, presumably, is because one cannot *adhere* to the enemy by anything less than a conscious object to do so. The modern dictionary definition of *adhere* recognizes such a connection between the adherent and the person who receives the adherence, as to "give support or maintain loyalty."[122] And Samuel Johnson's dictionary of 1755 defined *adhere* primarily as "sticking to," or "holding together," but also as "[t]o remain firmly fixed to a party, person, or opinion."[123] There is, therefore, support in English usage for the Court's understanding of the mental state that accompanies one's adherence to the enemy. Of course, one could argue that *Cramer* and *Kawakita* make too much of the specific intent to betray as a corollary of "adhering," and that treason could be found with something less than specific intent to betray America. For example, one might argue that the constitutional text stipulates only that one "adheres" to the enemy when he aids and comforts them. Therefore, the argument goes, so long as he actually gives aid and comfort, it matters not whether he intends specifically to betray the United States or simply desires some firm connection to a different group or idea, nor would it matter whether he gives aid and comfort only knowingly (in the sense that he is aware that is aiding an enemy of the United States), or even recklessly (in the sense

---

120 *Morrissette,* 342 U.S. at 252-53.

121 *Cramer*, 325 U.S. at 30.

122 *See* MERRIAM-WEBSTER DICTIONARY 14 (10th ed. 2002).

123 A DICTIONARY OF THE ENGLISH LANGUAGE: A DIGITAL EDITION OF THE 1755 CLASSIC BY SAMUEL JOHNSON 81 (1755) (Brandi Besalke, ed.), *available at*
http://johnsonsdictionaryonline.com/?page_id=7070&i=81.

that he is subjectively at fault for consciously choosing a course of conduct in which there is a substantial risk that he will aid and comfort the enemy). In any of these scenarios, so long as he remains fixed to an enemy in some way, he is by definition adhering to the enemy and has committed treason as the Constitution describes it. In this way, the law of treason still resists strict liability and maintains some substantial mens rea to accompany the relevant overt act, but is not what we would think of as a specific intent crime. If we do not accept "adhering" as necessarily requiring the specific intent to betray, then this reading of the Treason Clause seems plausible.

Hurst's work on treason also reached the conclusion that a specific intent to betray is an element of treason, and cites early cases rejecting guilt for treason based on a lack of intent to betray, yet even Hurst acknowledges authority to the contrary.[124] Hurst alludes only briefly to the disagreement in a footnote that compares the law of treason to the law of attempt, which requires the specific intent to carry out the target crime.[125] Hurst is correct that this is the general approach to attempt mens rea. But, for one thing, federal criminal law contains no general attempt statute, so there is no congressional enactment to which we can look to draw the comparison. Also, Hurst appears to be describing Levying War Treason, not Adherence Treason.[126] It is true that the specific intent would be the same for criminal liability under either theory, but because he discusses that specific intent as deriving from the natural betrayal of allegiance that would exist when levying war against one's country, he does not consider, as *Cramer* does, whether the specific intent to betray constitutes a natural reading of the word "adhering."[127] Indeed, he concedes that *Cramer* is ambiguous about the specific intent.[128] Finally, if Hurst was looking for a criminal law analogue to bolster the requirement of a specific intent, attempt seems to be the wrong analogue to Adherence Treason because the giving of aid and comfort with the

---

[124] *See* HURST, *supra* note 12, at 193-203.
[125] *Id.* 222-23 n.25.
[126] *See id.* at 193 (discussing "intent" in the context of levying war).
[127] *See Cramer*, 325 U.S. at 30.
[128] *See* HURST, *supra* note 12, at 193, 202.

requisite intent would complete the crime, thus taking it out of the law of attempts.

I would suggest still another way of thinking about the Treason Clause, and why it requires this kind of "intent," or purpose (or, as discussed previously, *motive*) to betray. Treason has been described as an "outlier" in criminal law, at least in the sense that it does not retain the structure of modern criminal law.[129] If that is true, then there is little reason to think it should employ the general parts of crime (actus reus, mens rea, causation) in the ways that modern criminal law would. And yet, if we consider the constitutional text closely, we see that Adherence Treason (as opposed to Levying War Treason) bears much resemblance to the law of complicity, and particularly the law of accomplice liability. This is not to say that one can be an accomplice to treason or that treason prosecutions can be based upon a theory of derivative liability. At common law, which applied the law of parties – now overwhelmingly abolished in American criminal law, but with which the Framers would have been familiar – treason was not among the crimes to which the law of parties applied.[130] Blackstone, in fact, reminds us that all who commit treason are principals.[131] Of course, that would be functionally true under existing federal criminal law as well, as it explicitly treats aiders and abettors as principals.[132] My point, rather, is merely to explain that there is symmetry between the law of Adherence Treason and the law of complicity.

In our criminal law, we understand that when X aids D in the commission of a crime, with the purpose of facilitating D's completion of the crime, then X is guilty of the underlying crime on the theory of accomplice liability.[133] Modern penal codes have worked some variation into this model, but the model itself prevails throughout American criminal law.[134] Of

---

[129] *See* Fletcher, *supra* note 14, at 1619.

[130] *See* DRESSLER, *supra* note 34, §30.03[A][1], at 460.

[131] *See* 4 WILLIAM BLACKSTONE, COMMENTARIES *35.

[132] *See* 18 U.S.C. § 2(a) (2012).

[133] *See* LAFAVE, *supra* note 50, §13.2, at 708 ("It may generally be said that one is liable as an accomplice to the crime of another if he (a) gave assistance or encouragement or failed to perform a legal duty to prevent it (b) with the intent thereby to promote or facilitate commission of the crime.").

[134] *See id.* §13.1(e), at 706-07.

course, the mental state required for accomplice liability is a subject of considerable debate,[135] and I do not purport to answer here the many questions that this debate raises. Nonetheless, it is fair to conclude that a consistent theme of the prevailing legal model is that, to be guilty as an accomplice, the one providing aid must provide it with the purpose of facilitating or promoting or encouraging the commission of the target offense, as well as with the mental state required by the target offense.[136] These are the so-called dual intents of accomplice liability.[137]

This is true under existing federal law, as well. Federal accomplice liability is governed by statute, section 2 of Title 18, which provides that "[w]hoever commits an offense against the United States or aids, abets, counsels, commands, induces, or procures its commission, is punishable as a principal."[138] Although the federal law of accomplice mens rea has been uneven, it has been generally agreed that the defendant must "intend" that the target crime be committed (though, again, there is considerable dispute about what "intent" means in this context – whether it requires the purpose that the target crime be committed, or simply knowledge that the assistance will aid the commission of the target crime).[139] In Judge Hand's words, the aider and abettor must have "associated himself with the venture, participated in it as in something he wished to bring about, and sought by his actions to make it succeed."[140] The Supreme Court, in fact, recently reaffirmed

---

[135] *Id.* §13.2(b), at 712-13. *See also* Baruch Weiss, *What Were They Thinking?: The Mental States of the Aider and Abettor and the Causer Under Federal Law*, 70 FORDHAM L. REV. 1341 (2002) (analyzing federal case law); John F. Decker, *The Mental State Requirement for Accomplice Liability in American Criminal Law*, 60 S.C. L. REV. 237 (2008) (analyzing various state law approaches); Grace Mueller, Note, *The Mens Rea of Accomplice Liability*, 61 S. CAL. L. REV. 2169, 2172 (1988) (discussing various theories).

[136] *See* DRESSLER, *supra* note 34, § 30.05, at 469-70.

[137] *Id.* at 469.

[138] 18 U.S.C. § 2(a) (2012).

[139] *See* LAFAVE, *supra* note 50, § 13.2(b)-(d), at 712-18.

[140] United States v. Peoni, 100 F.2d 401 (2nd Cir. 1938). The *Peoni* decision has been subject to question. *See, e.g.*, Stephen P. Garvey, *Reading* Rosemond, 12 OHIO ST. J. CRIM. L. 233, 239 n.23 (2014); Weiss, *supra* note 135, at 1424.

this standard and its kinship to the common law of accomplice liability.[141] Moreover, even under the law of accomplice liability, knowledge does not foreclose a finding of intent. Courts can sometimes infer intent from knowledge.[142] And to complicate matters further, there is authority, in federal criminal law as well, for the proposition that accomplice liability can be found where the accomplice simply has knowledge that her aid will facilitate a crime.[143] Again, though, the point is not to resolve the debate over mens rea of federal accomplice liability. The point, rather, is that because the constitutional text speaks in terms of "aiding" another (the enemy), there is a natural relationship between the Treason Clause and the law of accomplice liability, the law of aiding another. Understanding Adherence Treason as a species of complicity – or at least as a close cousin – may help improve our understanding of the Treason Clause and how it functions in the modern world of criminal law.

Both *Cramer* and *Kawakita*, in fact, use language that only amplifies the sounds of complicity doctrine that accompany the Treason Clause. In *Cramer*, the Court speaks in terms that remind us of the dual intents.[144] And although Hurst criticized the *Cramer* Court's conclusion that the

---

[141] *See* Rosemond v. United States, 134 S. Ct. 1240 (2014). This is not to say that *Rosemond* definitively answers problems related to the mens rea of accomplice liability. *See* Garvey, *supra* note 140, at 238-50.

[142] A well-known case on this subject (though it appears in the conspiracy context) is People v. Lauria, 251 Cal. App. 2d 471 (Cal. Dist. Ct. App. 1967), in which the operator of telephone answering service permitted participants in a prostitution ring to use his service, knowing that the service was used for this purpose. The court explained the circumstances under which intent may be inferred from knowledge, *id.* at 478-81, but that none of those circumstances existed in Lauria's case because he had no special interest or stake in the success of the prostitution venture. *Id.* at 482-83.

[143] *See, e.g.*, United States v. Fountain, 768 F.2d 790, *modified*, 777 F.2d 345 (7th Cir. 1985); United States v. Campisi, 306 F.2d 308 (2nd Cir. 1962). *See also* Weiss, *supra* note 135, at 1396-1409 (analyzing federal case law on knowledge).

[144] *Cramer*, 325 U.S. at 31.

treasonous overt act must actually aid the enemy,[145] that particular reading of the Treason Clause – whatever the other shortcomings of the *Cramer* opinion – would at least be consistent with the common law understanding of aid for accomplice liability, which required that the accomplice's aid in fact assist the principal.[146] Moreover, in *Kawakita*, the Court explained that Adherence Treason does not require that the overt act be one that turns the tide in the enemy's efforts, or even that it be one of great significance to the enemy.[147] The overt act can be insubstantial and have little or no ultimate effect on the war effort against the United States.[148] So long as the aid that the traitor provides would, at a minimum, embolden the enemy in its efforts, the aid is sufficient for treason (when joined with the relevant treasonous intent).[149] A parallel principle exists in the law of accomplice liability. The aid need not be significant.[150] Rather, even trivial assistance or even mere psychological encouragement, combined with the relevant specific intent, is sufficient for guilt on a theory of accomplice liability.[151]

The Snowden affair offers an example of how this principle functions. Because of the scope of the information that he disclosed, and the likelihood that this information reached an American enemy (ISIS, al Qaeda, etc.), it is certainly plausible to think that the disclosure aided them.[152]

---

[145] *See* HURST, *supra* note 12, at 210. *See also* Crane, *supra* note 13, at 654-56 (surveying scholarly criticism of Justice Jackson's *Cramer* opinion).

[146] *See* DRESSLER, *supra* note 34, § 30.04[B][1], at 467.

[147] *See Kawakita*, 343 U.S. at 738.

[148] *Id.* The Court also cited *Haupt*, saying that "harboring the spy in *Haupt v. United States* . . . was also insignificant in the total war effort of Germany during the recent war. Yet it was a treasonable act." *Id.*

[149] *See* LAFAVE, *supra* note 50, § 13.2(a), at 708-09 (describing how encouragement may allow guilt on accomplice liability theory).

[150] *See* United States v. Bennett, 75 F.3d 40, 45 (1st Cir. 1996).

[151] *See* DRESSLER, *supra* note 34, § 30.04[B][1], at 467. The law of trivial assistance has come under fire. *See* Joshua Dressler, *Reforming Complicity Law: Trivial Assistance as a Lesser Offense?,* 5 OHIO ST. J. CRIM. L. 427 (2008).

[152] *See* James Gordon Meek, et al., *Intel Heads: Edward Snowden Did 'Profound Damage' to U.S. Security*, ABC NEWS (Jan. 29, 2014), *available at* http://abcnews.go.com/Blotter/intel-heads-edward-snowden-

Even if the disclosure did not directly result in any American casualties, or even have any significant role in an enemy attack, the disclosures at least could have emboldened the enemy or strengthened the enemy's fortitude in planning or perhaps even executing an attack. And yet, again, in the absence of an intent that the enemy launch a successful attack, the aid that the disclosures provided would not be treasonous aid and comfort. The Snowden example, in fact, shows how the overlap of treason law with complicity law would resolve the knowledge/purpose debate. That is, even if Snowden was aware (had knowledge) that his actions would aid the enemy (and this is a fair bet), he still would not be guilty of treason because he lacked the specific purpose to betray.

But think about a different example. Imagine an American citizen who decides to join the cause of, for instance, al Qaeda or ISIS. He or she then communicates information digitally – such as via YouTube, Twitter, email, or posted on a personal blog – so that the enemy could have easy access to it, indeed, with the hope that the enemy would gain access to it for purposes of planning an attack or doing some harm to America or its security interests. This could be sensitive national security information to which the person has access (like the information Snowden disclosed), or it could be other information that may benefit those enemy groups in planning or executing an attack. It could even be information pledging support for the terrorist cause and a hope for the killing of Americans, or the destruction of the United States. If the enemy never sees or receives the communication, then even though the citizen intended to betray America, a treason prosecution is likely barred. It offered no aid. As in the common law of accomplice liability, attempted aid is insufficient for proving guilt, unless the attempted aid is known to the principal actor and thus serves as encouragement.[153] The overt act must actually offer some aid and comfort.

The Constitution does not mandate *significant* aid and comfort, however. So if the enemy receives and sees or hears

---

profound-damage-us-security/story?id=22285388 (describing views of James Clapper, Director of National Intelligence, and John Brennan, CIA Director).

[153] *See* LAFAVE, *supra* note 50, §13.2(a), at 712.

the communication, and even if the information merely encourages them or bolsters their fortitude to harm America or is otherwise only minimally helpful to their cause, this is arguably treasonous (assuming, of course, satisfaction of the constitutional proof requirements).[154] The same could be said of Americans who have taken affirmative steps to not only indicate their support for ISIS, but to personally, and more directly, assist ISIS.[155] Even if those citizens never actually reached a destination in which they would fight alongside other ISIS cohorts, the key question is whether the steps they have taken to join ISIS fighters would encourage ISIS in its mission. These are somewhat closer cases, at least where the person has not actually reached the point of actual fighting or other direct aid beyond expressions of support or encouragement for the terrorists. Material support for terrorism (or conspiracy to provide it, or attempt to provide it) offers a clearer legal basis for prosecution,[156] and indeed, that has been the charge of choice for federal prosecutors in those cases.[157] But many of the acts that constitute material support

---

[154] *See Kawakita*, 343 U.S. at 738. *See also Bollman*, 8 U.S. (4 Cranch) at 126 ("[i]f war actually be levied, . . . all those who perform any part, however minute, or however remote from the scene of action, and who are actually leagued in the general conspiracy, are to be considered as traitors.").

[155] *See*, *e.g.*, *More young Americans arrested for joining ISIS*, AOL (Mar. 4, 2015, 11:10 PM), http://www.aol.com/article/2015/03/04/more-young-americans-arrested-for-joining-isis/21149844/ (noting comments by James Clapper that about 180 Americans have traveled to Syria to fight alongside ISIS); Elizabeth Whitman, *Americans Joining ISIS: Arrests Suggest Young Muslims Lured by Social Media*, INTERNATIONAL BUSINESS TIMES (Feb. 25, 2015, 3:22 PM), http://www.ibtimes.com/americans-joining-isis-arrests-suggest-young-muslims-lured-social-media-1828286 (noting various citizens or American residents who have tried to join ISIS); *How many Americans have joined ISIS?,* CBS NEWS (Aug. 22, 2014, 2:09 PM), http://www.cbsnews.com/news/how-many-americans-have-joined-isis/.

[156] *See* 18 U.S.C. §§ 2339A, 2339B (2012).

[157] *See* Press Release, U.S. Dept. of Justice, Philadelphia Woman Arrested for Attempting to Provide Material Support to ISIL (Apr. 3, 2015); Press Release, U.S. Dept. of Justice, Madison, Wisconsin Man Charged with Attempting to Provide Material Support to ISIL (Apr. 9, 2015); Press Release, U.S. Dept. of Justice, Fourth Brooklyn, New

would also likely constitute "aid and comfort" for purposes of Adherence Treason.[158] So prosecutors should not rule out the possibility of treason, based on the complicity theory articulated here.[159] Notice, though, how these scenarios differ significantly from the Snowden affair – they, unlike the Snowden affair, couple assistance (and an intent to render the assistance) with an intent to betray.

Though the parallels are there, the Court – in its few treason cases – has not discussed the law of Adherence Treason in these accomplice liability terms. And the parallels are admittedly imperfect, chiefly because we do not prosecute Adherence Treason on a theory of complicity. Accomplice liability is derivative, and treason liability is always direct. Adherence, with the provision of aid and comfort, *is* the crime. Nonetheless, we see that there are important parallels between Adherence Treason and complicity law – especially the law of accomplice liability, an older version of which the Framers would have known – that may explain the outcomes in both *Cramer* and *Kawakita* and help us better approach future problems involving the nature of one's aid to the enemy and the mental state that must accompany that aid. This is especially true at time when, thanks to digital technology accessible anywhere in the world, aiding or encouraging the enemy can be easy, instantaneous, and potentially quite harmful to American institutions and interests.

IV. CONCLUSION

Whatever else Edward Snowden is guilty of, he is most likely not guilty of treason. That does not mean that we, and our political leaders with us, should not condemn his conduct. Rather, it simply means that we should endeavor to be more accurate in our use of treason as serious political rhetoric and more conscientious about developing a complete – or, as

---

York Resident Charged with Attempt and Conspiracy to Provide Material Support to ISIL (Apr. 6, 2015).

[158] *See* 18 U.S.C. §2339A(b) (2012) (broadly defining "material support").

[159] *Cf.* Eichensehr, *supra* note 10, at 1503-05 (arguing that, in balancing advantages and disadvantages of treason prosecutions for assisting non-state actors, often the benefits will outweigh the risks).

complete as can be expected, given the complexity and nature of it – understanding of American treason law. American treason is supposed to be hard to prove, hard to prosecute, and hard to punish. Yet where it exists, as the Constitution defines it, federal prosecutors should be more ready to enforce it and to seek severe punishment for it. Modern technology and social media, and the demonstrated willingness of some Americans to join forces with modern terrorists, could make treason prosecutions more plausible than they have been in American history. As the Snowden affair reveals, however, treason against the United States requires that only with the confluence of a sufficiently guilty act and guilty mind devoted to betraying America will a treason prosecution represent a constitutionally acceptable legal response to conduct that harms American national security and the institutions of American government. Merely doing harm to American interests may be criminal, but it is not necessarily treasonous. This might make us inclined to broaden American treason, for broadening treason law might make it easier for us to allege and prove treason with respect to Americans who do harm to American institutions and interests by aiding our enemies. And it might make us feel better about having a criminal law that comports with our rhetorical and psychological sensibilities about disloyalty. But doing so would be inconsistent with the narrow and limited version of treason that the founding generation – which well understood the politics and consequences of disloyalty – not only desired, but provided in the constitutional text. Weakening the limits on American treason could undermine the delicate balance that the Constitution has struck to ensure sober use of the federal power to punish treachery against the Nation.

LINCOLN MEMORIAL UNIVERSITY
LAW REVIEW

VOLUME 3 FALL 2015

GOVERNMENT SECRETS:
THE PUBLIC'S MISCONCEPTIONS OF THE SNOWDEN DISCLOSURES

Melanie Reid[*]

"Secrets, silent, stony sit in the dark palaces of both our hearts: secrets weary of their tyranny: tyrants willing to be dethroned."
--James Joyce

I. INTRODUCTION

Human beings are curious by nature. We love to ask the "why" questions and would rather be privy to a secret than be kept in the dark. Not surprisingly, government conspiracy theories are quite popular.[1] It is much more

[*]Associate Professor of Law, Lincoln Memorial University-Duncan School of Law. I would like to thank Lauren Mullins for her invaluable research assistance, enthusiasm, thoughts and critiques on this topic.

[1] JFK (Warner Bros. 1991) (US Gross Box Office = $70,405,498) http://www.imdb.com/title/tt0102138/business?ref_=tt_dt_bus; CONSPIRACY THEORY (Warner Bros. 1997) (US Gross Box Office =

interesting to think part of the government was somehow involved in the assassination of President John F. Kennedy rather than believe the lone gunman theory, or that the government is covering up an alien invasion by storing UFOs and alien bodies at Area 51 in Roswell rather than believe no such thing exists.[2]

Thus, when Edward Snowden revealed that one of the government's most secretive agencies, the National Security Agency ("NSA"), previously nicknamed "No Such Agency," was keeping a huge secret from the American people and monitoring American citizens' phone calls, instant messaging, emails, documents kept in the "cloud," contact lists, metadata,[3] GPS data, etc., this became one of the greatest government conspiracy theories to contemplate since JFK and Roswell.

Is the NSA listening to my phone call right now? What if I say the word "president" or "al Qaeda," would they definitely be listening then? Or what if I "Google" one of these words? Would the NSA instantly watch what websites I am viewing?

Of course, it would be extremely difficult to keep such a large-scale government conspiracy under wraps. It seems

---

$76,081,498)
http://www.imdb.com/title/tt0118883/business?ref_=tt_dt_bus.

[2] Journalist Annie Jacobsen surmised that the UFOs and aliens found in Roswell, Nevada in 1947 were actually Russian children around 12-years-old with large heads and abnormally shaped, over-sized eyes that were the genetic experiments of Josef Mengele, a former German Nazi officer and physician in Auschwitz. ANNIE JACOBSEN, AREA 51: AN UNCENSORED HISTORY OF AMERICA'S TOP SECRET MILITARY BASE 2011. Soviet leader Joseph Stalin wanted to cause hysteria in America with the thought of "UFOs and an alien invasion." *Id.*

[3] Metadata, or transactional information, is collected as phone calls "are handed over, as is location data, call duration, unique identifiers, and the time and duration of all calls. The contents of the conversation itself are not covered." Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN, June 5, 2013,
http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. The "business records" provision of the PATRIOT Act (50 U.S.C. § 1861 (2014)) has been used as a legal justification for bulk collection of domestic telephone records. *Id.*

surprising that any top-secret classified government operation is kept a secret. Ben Franklin's famous quote, "[t]hree may keep a secret, if two of them are dead,"[4] might sound melodramatic but it rings true. Not much is kept secret anymore – in fact, there appears to be more and more disclosures as spies, whistleblowers, journalists, and insiders begin to share their knowledge and spread it throughout the internet. The public clamors it has a need-to-know in order to keep the government in check.

But what is it we need to know? Do we need to know the specifics as to how individual NSA collection programs work? Should the public know which communication methods are being intercepted by the NSA and thus compromised, or what foreign embassies and consulates are being surveilled both inside and outside of the U.S., or how electronic beacons are implanted within targeted electronic devices, or how the NSA taps into the telecommunications of service providers, or know about U.S. collection priorities against foreign countries?

Once the initial reporting on the Snowden leak began in June 2013, the media and public wanted to know more – what was the NSA collecting, what were they listening to, what were they doing with this information, who are they sharing this information with? The actual legalities and illegalities of certain NSA programs and collection of data became more blurred as the media focused on the wide-scale public outrage at the idea that the government was spying on its own citizens regardless of the legalities. The media emphasized the public's ever-increasing distrust of government and the intelligence community's (IC)[5] classified programs.

---

[4] Benjamin Franklin, *Poor Richard's Almanack* (1735), *available at* http://www.vlib.us/amdocs/texts/prichard35.html. A student of mine recently informed me this is also the theme to a show entitled, "Pretty Little Liars."

[5] "The Intelligence Community (IC) is a group of Executive Branch agencies and organizations that work separately and together to engage in intelligence activities that are necessary for the conduct of foreign relations and the protection of the national security of the United States." OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, U.S. NATIONAL INTELLIGENCE: AN OVERVIEW 7 (2011), *available at* http://www.dni.gov/files/documents/IC_Consumers_Guide_2011.

Now that the initial deluge of classified information from Snowden's leaks has been disclosed, the questions are two-fold: (1) are these expansive collection programs by the IC legal or illegal and (2) if legal, are these "whistleblower" disclosures justified given the resultant damage these leaks have caused to our national security and law enforcement's ability to prevent the commission of future crimes?

II. LEGALITY OF IC'S ACTIONS

What is difficult to determine from the recent media disclosures is what exactly is being collected, how is the information collected, at what point can communications be accessed and analyzed, who receives the analysis, and what is the legal justification for each step along this process. There is a significant distinction between authorizations to collect telephone caller identification record information, or "to" and "from" information on a particular email address, versus authorization to listen in on the content of such communications. If this distinction is not made clear, then the public can draw erroneous conclusions about alleged breaches of privacy based upon misinformation.

A. NSA'S BULK COLLECTION OF METADATA: SECTION 215

Snowden disclosed that the NSA is collecting the metadata from millions and even billions of phone calls and emails sent out every day, including Americans' emails and

---

pdf. Sixteen United States intelligence agencies comprise the IC and are under the Office of the Director of the National Intelligence: the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, the National Geospatial-Intelligence Agency, the Federal Bureau of Investigation (FBI) National Security Branch, the Drug Enforcement Administration (DEA) Office of National Security Intelligence, Department of Treasury Office of Intelligence and Analysis, Department of Energy Office of Intelligence and Counter-intelligence, State Bureau of Intelligence and Research, Department of Homeland Security Office of Intelligence and Analysis, and Army, Air Force, Coast Guard, Marine Corps, and Naval Intelligence. *See id*. at 9.

phone calls.[6] Metadata includes "much of the information that appears on a customer's telephone bill: the date and time of a call, its duration, and the participating telephone numbers" and can include the nature of "how the call was routed from one participant to the other through the infrastructure of the telephone companies' networks."[7]

The NSA was given this power when the PATRIOT Act was passed post-9/11.[8] Section 215 of the Act allows the government to obtain a Foreign Intelligence Surveillance Court (FISC or FISA court) order every ninety days requiring third parties (including telecommunications providers) to hand over any records or other "tangible thing" if deemed "relevant" to "any investigation to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities."[9]

The NSA utilized this "Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations" power to justify their bulk telephone records collection program.[10] The NSA began to collect metadata from all sorts of third parties, including telecommunications carriers and internet providers, in order to have the information close

---

[6] GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE 30-32 (2014).

[7] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 8, 21 (Jan. 23, 2014) [hereinafter PCLOB TELEPHONE RECORDS REPORT], *available at* http://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

[8] *Id.*

[9] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, sec 208(1), Pub. L. No. 107-56, 115 Stat. 272 [hereinafter PATRIOT Act] (codified in scattered titles of U.S.C.), *available at* http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf., at sec. 215. *See also* BRENNAN CENTER FOR JUSTICE, ARE THEY ALLOWED TO DO THAT? A BREAKDOWN OF SELECTED GOVERNMENT SURVEILLANCE PROGRAMS 1 http://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf.

[10] PCLOB TELEPHONE RECORDS REPORT, *supra* note 7, at 8.

at hand when it came time to conduct a targeted search.[11] The NSA stores these collected telephone records in a centralized database.[12] Before an analyst can access the database and search for a specific number or selection term, "one of twenty-two designated NSA officials must first determine there is a reasonable, articulable suspicion that the number is associated with terrorism."[13] Once the analyst gains approval, he or she "may run queries that will return the calling records for that seed [number], and permit 'contact chaining' to develop a fuller picture of the seed's contacts. Contact chaining enables analysts to retrieve not only the numbers directly in contact with the seed number ("the first hop"), but also numbers in contact with all first hop numbers (the "second hop"), as well as all numbers in contact with all second hop numbers (the "third hop")."[14]

The government's argument is that one cannot investigate and prevent terrorist attacks without real-time access to metadata to determine who is contacting whom and when. "When the NSA identifies communications that may be associated with terrorism, it issues intelligence reports to other federal agencies, such as the FBI, that work to prevent terrorist attacks."[15] It is difficult to predict when attacks may occur, even more so if one hand is tied behind the IC's back when not given the ability to follow a target's phone number trail wherever that might lead.

Critics of section 215 argue that by permitting intelligence agencies, specifically the NSA, to collect metadata from a variety of third parties, section 215 allows the government to get a whole picture of a person by searching one's "financial, library, travel, video rental, phone, medical, church, synagogue, and mosque records . . . providing the government says it's trying to protect against terrorism."[16]

---

[11] BRENNAN CENTER FOR JUSTICE, *supra* note 9, at 1-2.
[12] PCLOB TELEPHONE RECORDS REPORT, *supra* note 7, at 8.
[13] *Id*. at 8-9.
[14] *Id*. at 9.
[15] *Id*. at 8.
[16] Emma Roller, *This Is What Section 215 of the Patriot Act Does*, SLATE (June 7, 2013, 1:17 PM), http://www.slate.com/blogs/weigel/2013/06/07/nsa_prism_scandal_what_patriot_act_section_215_does.html.

Metadata, "if properly exploited, could yield more valuable information than recordings of the phone calls or email messages themselves."[17]

Critics further argue that "[i]t is difficult to believe that the phone records of millions of Americans are actually 'relevant' to a specific terrorist or foreign intelligence investigation. Nor does Section 215 appear to allow the government to collect first and determine relevance later, which is what the government claims it is doing."[18]

In January 2014, the Privacy and Civil Liberties Oversight Board (PCLOB)[19] issued a report after reviewing the NSA's bulk collection of phone records. The PCLOB found the bulk collection of phone records failed to comply with Section 215 and therefore should be terminated or significantly revised.[20] The PCLOB determined (1) the bulk telephone records acquired had "no connection to any specific FBI investigation at the time of their collection;" (2) since the records are collected in bulk, they are not "relevant" to a particular investigation as required under section 215; (3) requiring telephone companies to furnish new call records on a daily basis is not permitted under section 215 nor FISA; and (4) section 215 only permits the FBI and not the NSA to obtain records relevant to a terrorism or foreign intelligence investigation.[21]

That same month, President Obama made his own comments regarding the section 215 program, stating he would continue to allow government use of bulk phone records while they attempt to come up with an alternative

---

[17] SHANE HARRIS, THE WATCHERS: THE RISE OF AMERICA'S SURVEILLANCE STATE 204-05 (Penguin Books, 2011).

[18] BRENNAN CENTER FOR JUSTICE, *supra* note 9, at 3.

[19] The Privacy and Civil Liberties Oversight Board (PCLOB) was established in 2004 by the Intelligence Reform and Terrorism Prevention Act of 2004. In 2007, the 9/11 Commission Act restructured the Board requiring that all five members be appointed by the President. *See* 42 U.S.C.A. § 2000(e)(e) (2012 & Supp. 2014). As a result, the Board did not fully exist until June 2013, after the Senate confirmed members to resume operations. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, http://www.pclob.gov/about-us (last visited Aug. 23, 2014).

[20] PCLOB TELEPHONE RECORDS REPORT, *supra* note 7, at 10.

[21] *Id.*

solution "without the government holding this metadata itself" and would require the agency to get court approval prior to accessing the metadata.[22] The NSA would also no longer be able to access records that go beyond two persons removed from the original query.[23]

In response to these findings, in May 2014, the House passed the USA Freedom Act[24] which focuses on the NSA's call-records program in which the agency retains billions of records for all phone calls made from or to the United States. Under the legislation, telecommunications companies would retain those records, and the NSA would only have access to specific information about targeted individuals under court orders.[25] A year later, due to inaction by the Senate, the bulk collection program under section 215 was allowed to expire on June 1, 2015.[26] The Senate then approved the USA Freedom

---

[22] Transcript of President Obama's Jan. 17 Speech on NSA Reforms, WASH. POST, Jan. 17, 2014, http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

[23] *Id*.

[24] USA Freedom Act, H.R. 3361, 113th Cong. (2013-2014), *available at* https://beta.congress.gov/bill/113th-congress/house-bill/3361.

[25] *Id*. The bill "[r]equires the FBI to include in such tangible thing applications a specific selection term to be used as the basis for such production." *Id*. A "specific selection term" is "a term specifically identifying a person, entity, account, address, or device" that is "used by the government to limit the scope of the information or tangible things sought pursuant to the statute." *Id*. In each application requesting call detail records (i.e., telephone numbers and time or duration of a call), the FBI must show "(1) reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term are relevant to such investigation; and (2) facts giving rise to a reasonable, articulable suspicion that such specific selection term is associated with a foreign power or an agent of a foreign power." *Id*.

[26] Opinion and Order *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Docket No. BR 15-75, Foreign Intelligence Surveillance Court, June 29, 2015 at 2. *See also* Erin Kelly, *Here's what happens now that the Patriot Act Provisions Expired*, USA Today, June 1, 2015, http://www.usatoday.com/story/news/nation/2015/05/31/patriot-act-expires-senate-stalemate/28260905/.

Act on June 2nd, and the revised Section 215 program which effectively eliminates bulk collection will continue until December 15, 2019.[27] The USA Freedom Act allows the bulk collection of telephone metadata for only a 180 day transition period (until November 29, 2015) during which such collection could continue.[28]

B. NSA'S MONITORING OF CONVERSATIONS: FISA AND SECTION 702

Section 215 of the PATRIOT Act addresses the bulk collection of telephone records, and the FISA Amendments of 2008 (FAA) address the collection and subsequent analysis of the content of telephone and internet communications.[29] The FAA (also known as section 702) has been utilized to allow the NSA to work with electronic communication service providers "to copy, scan, and filter internet and phone traffic coming through their physical infrastructure" and compel the disclosure of the content of such communications so long as it targets foreign persons reasonably believed to be located outside the United States.[30] No particular warrant is required in that instance. The targeting of the non-U.S. person on foreign soil must be conducted in order to acquire foreign

---

[27] Opinion and Order *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Docket No. BR 15-75, Foreign Intelligence Surveillance Court, June 29, 2015 at 2-3 (citing to USA FREEDOM Act § 705(a)).

[28] Opinion and Order *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Docket No. BR 15-75, Foreign Intelligence Surveillance Court, June 29, 2015 at 10-11 (citing to section 109(a) of the USA FREEDOM Act).

[29] H.R. 6304, 110th Cong. (2007-2008), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-110hr6304enr/pdf/BILLS-110hr6304enr.pdf.

[30] ELECTRONIC FRONTIER FOUNDATION, COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION REGARDING SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE AMENDMENTS ACT TO THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD 8 (Apr. 22, 2014), *available at* https://www.eff.org/files/2014/04/22/eff_pclob_comments_11_april_2014.pdf; *See also* H.R. 6304, 110th Cong. (2007-2008), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-110hr6304enr/pdf/BILLS-110hr6304enr.pdf.

intelligence information as defined in FISA, and the NSA must obtain approval from the FISA court as to their targeting and minimization procedures prior to collection to make sure U.S. persons are not inadvertently intercepted.[31]

Unfortunately, it is virtually impossible to separate the collection of phone and internet communications of strictly foreign persons from U.S. persons if the foreign person is communicating with a U.S. person.[32] These communications are also potentially being copied and stored in a searchable database.[33] Information on U.S. persons may incidentally be collected if that U.S. person communicates with a non-U.S. person that is being targeted or two non-U.S. persons discuss the U.S. person.[34] Or, a U.S. person's conversation may inadvertently be collected by mistake if erroneously targeted by the NSA and thought to be a non-U.S. person.[35] In the case of inadvertent collection, the communications must be destroyed.[36]

The Privacy and Civil Liberties Oversight Board (PCLOB) approved of the Section 702 program in its report dated July 2, 2014, stating:

---

[31] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 6 (July 2, 2014) [hereinafter PCLOB SECTION 702 REPORT], *available at* https://www.nsa.gov/civil_liberties/_files/pclob_section_702_report.pdf. "The targeting procedures govern how the executive branch determines that a particular person is reasonably believed to be a non-U.S. person located outside the United States, and that targeting this person will lead to the acquisition of foreign intelligence information. The minimization procedures cover the acquisition, retention, use, and dissemination of any non-publicly available U.S. person information acquired through the Section 702 program." *Id*. at 6-7. "For example, the NSA's minimization procedures require that queries of Section 702-acquired information be designed so that they are 'reasonably likely to return foreign intelligence information.'" *Id*. at 8.

[32] JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA 304 (Anchor Books, 2009).

[33] *Id*.

[34] PCLOB SECTION 702 REPORT, *supra* note 28, at 6.

[35] *Id.*

[36] *Id.*

> [t]he Section 702 program has enabled the government to acquire a greater range of foreign intelligence than it otherwise would have been able to obtain – and to do so quickly and effectively. Compared with the "traditional" FISA process under Title I of the statute, Section 702 imposes significantly fewer limits on the government . . . [t]he program has proven valuable in the government's efforts to combat terrorism as well as in other areas of foreign intelligence. . . . [m]onitoring terrorist networks under Section 702 has enabled the government to learn how they operate, and to understand their priorities, strategies, and tactics.[37]

While the core of the section 702 program was deemed to be "reasonable" under Fourth Amendment law, the PCLOB set forth additional proposals to address their concerns about

> the unknown and potentially large scope of the incidental collection of U.S. persons' communications, the use of "about" collection to acquire Internet communications that are neither to nor from the target of surveillance, and the use of queries to search for the communications of specific U.S. persons within the information that has been collected.[38]

On June 19, 2014, the House passed a bill that includes an amendment which bars the NSA, the CIA, and others in the IC from actually examining the communications of Americans that were collected into databases created to target foreigners.[39] Critics have called this technique the "backdoor

---

[37] *Id.* at 9-10.
[38] PCLOB TELEPHONE RECORDS REPORT, *supra* note 7, at 9.
[39] H.R. 5016, 113th Cong. (2013-2014), *available at* https://beta.congress.gov/bill/113th-congress/house-bill/5016/amendments.

search loophole."[40] "The bill also prohibits the government from requiring a private company to alter its software to allow clandestine surveillance."[41]

C. LEGAL CONCLUSIONS AS TO IC ACTIONS

In summary, upon review of FISA, the FAA, and the PATRIOT Act, it would be lawful for the NSA to monitor electronic communications of foreign persons reasonably believed[42] to be located overseas without any type of warrant. However, if that person is a "U.S. person" or that foreign person was to communicate with a person located in the United States, the NSA would need to apply for a FISA warrant. The difficulty is in determining where the particular person is located at the time of the call. While the law does not allow the intentional monitoring of U.S. persons, the FISC approves minimization procedures to limit the amount of information about U.S. persons that is intercepted, retained, and disseminated. Hence, the IC's monitoring of content in communications is legal.

On the other hand, the legality of the NSA's collection of metadata is uncertain. While the NSA had previously used section 215 of the PATRIOT Act to justify its bulk records

---

[40] Charlie Savage, *House Votes to Curb N.S.A. Scrutiny of Americans' Communications*, NY TIMES (June 20, 2014), http://www.nytimes.com/2014/06/21/us/politics/house-votes-to-curb-nsa-scrutiny-of-americans-communications.html.

[41] Andrew Rosenthal, *The House Actually Did Something About Warrantless Surveillance*, TAKING NOTE: THE EDITORIAL PAGE EDITOR'S BLOG (June 20, 2014, 1:30 PM), http://takingnote.blogs.nytimes.com/2014/06/20/the-house-actually-did-something-about-warrantless-surveillance/.

[42] "[T]he NSA has reportedly interpreted that to mean that it need only ensure '51 percent confidence of the target's 'foreignness.'" BRENNAN CENTER FOR JUSTICE, *supra* note 9, at 3; *See also* Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, WASH. POST (June 6, 2013), http://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.

collection program,[43] it is now clear that the NSA has been collecting more than foreign persons' metadata and metadata not necessarily relevant to a terrorism or foreign intelligence investigation.[44] Regardless, the bulk data collection of business records and other tangible things, as we know it, will terminate after November 29, 2015.[45] After such date, the IC will have to furnish "specific selection term[s]" to the FISC before being granted access to such metadata from third party communications providers.[46] However, at the time of the Snowden leak, both the monitoring of content and the bulk records collection program were legally justified.

III. SNOWDEN'S REASONS FOR DISCLOSURE VERSUS DAMAGE DONE TO NATIONAL SECURITY

A. BULK COLLECTION AND KEEPING THE INTERNET "FREE"

Snowden's real complaint seems to boil down to the NSA's collection of metadata – not the subsequent analysis of this data because targeting and minimization procedures have been put in place to avoid bulk *analysis* of the data collected. Therefore, Snowden is concerned about the *potential* for abuse in the collection of metadata not necessarily current abuse of power now that this data is in the hands of the NSA.

---

[43] 50 U.S.C.A. § 1861(a)(1) (2003 & Supp. 2014).

[44] Barton Gellman et al., *In NSA-intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are,* WASH. POST (July 5, 2014), http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html?hpid=z1.

[45] Opinion and Order *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Docket No. BR 15-75, Foreign Intelligence Surveillance Court, June 29, 2015 at 18.

[46] Opinion and Order *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Docket No. BR 15-75, Foreign Intelligence Surveillance Court, June 29, 2015 at 10 (citing to USA FREEDOM Act § 103(b), amending FISA § 501(c)).

Snowden has given several interviews and written manifestos explaining why the public needs to know the specifics as to what the NSA is collecting and how they are collecting it. In Snowden's eyes, only with the public's input can true regulation and accountability take place.[47] Apparently, congressional oversight committees, the FISC, the Department of Justice, internal agency auditing and monitoring, and oversight from the Executive branch is not enough. It bears reminding that the previously described collection and surveillance programs are regulated – by Congress, by the FISC, by the Department of Justice and by oversight lawyers within intelligence agencies themselves.[48]

Snowden wants to keep the internet free from NSA collection – so that those who grow up on the internet feel free to explore, make mistakes, and express themselves without fear that anyone is watching.[49] Unfortunately, regardless of whether the NSA is watching, others are and will always be watching. Private companies make it their mission to collect as much information as possible on individual consumers and sell it to the highest commercial bidder. Criminals both overseas and in our own back yard who want to steal our information are monitoring and exploiting the Internet as well. Director of the FBI, James Comey, recently stated,

---

[47] GREENWALD, *supra* note 6, at 13, 30-31.

[48] At a recent debate, former CIA director James Woolsey stated,

> I have seen, either from in the Executive Branch, or as a private citizen interested in these issues and following them, the oversight personnel capabilities, numbers of offices, numbers of people involved in overseeing the American system of intelligence is truly awesome. There is no country anywhere in the world that has the massive oversight from legislative, judicial, and executive sides and functions over their intelligence systems. Nobody is even close to the United States.

Transcript of INTELLIGENCE SQUARED U.S. debate, *Snowden was justified*, (Feb. 12, 2014), *available at* http://intelligencesquaredus.org/images/debates/past/transcripts/021214%20Snowden.pdf.

[49] GREENWALD, *supra* note 6, at 46-47.

> I think there's something about sitting in front of your own computer working on your own banking, your own health care, your own social life that makes it hard to understand the danger (of third party surveillance, cybercrime, and cyber-attacks on companies and individuals on the internet). I mean, the Internet is the most dangerous parking lot imaginable. But if you were crossing a mall parking lot late at night, your entire sense of danger would be heightened. You would stand straight. You'd walk quickly. You'd know where you were going. You would look for light. Folks are wandering around that proverbial parking lot of the Internet all day long, without giving it a thought to whose attachments they're opening, what sites they're visiting. And that makes it easy for the bad guys.[50]

The Internet, unfortunately, will never be free from surveillance. Even if our government is not monitoring the Internet, there will always be a myriad of bad actors that do. Foreign Intelligence Services target the Internet to collect positive intelligence and steal trade secrets, cyber criminals hack into our private e-mails and steal personal identification information, terrorist organizations promote jihad and the destruction of our cyber infrastructure.

More importantly, do we want our government to be proactive and attempt to prevent or disrupt terrorist attacks before they take place? If the answer is yes, then we need to provide federal law enforcement with a requisite amount of surveillance tools to be able to accomplish this mission.

---

[50] Transcript of Interview by Scott Pelley with James Comey, Oct. 5, 2014, *available at* http://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/.

B. BULK COLLECTION AND THE *POTENTIAL* FOR ABUSE OF POWER

Snowden's argument for public disclosure would be much stronger if he could point to specific abuses of power that would liken current NSA activities to those abuses disclosed in the 1970's during the Church Committee hearings. The Church Committee discovered that the IC had illegally gathered information and compiled files on communists in the 1950s and civil rights groups and Vietnam War protesters in the 1960s.[51] These findings resulted in a significant overhaul in IC oversight and accountability and the passage of the Foreign Intelligence Surveillance Act (FISA) of 1978 in order to prevent future abuse of power by the IC.[52]

In addition to his concerns about NSA spying on Americans through its bulk collection programs, Snowden also disclosed examples of individual government employees who abused the power and responsibility placed in their hands. This abuse of power was illegal, and the offenders should have faced criminal or severe administrative penalties, but their behavior in many instances was either condoned or overlooked. In one article, Snowden is quoted as saying,

> Many of the people searching through the haystacks were young, enlisted guys, 18 to 22 years old. They've suddenly been thrust into a position of extraordinary responsibility, where they now have access to all your private records. In the course of their daily work, they stumble across something that is completely unrelated in any sort of necessary sense – for example, an intimate nude photo of someone in a sexually compromising situation. But they're extremely attractive. So what do they do? They turn around in their chair and they show a co-

---

[51] UNITED STATES SENATE, *Senate History: January 27, 1975 Church Committee Created*, http://www.senate.gov/artandhistory/history/minute/Church_Committee_Created.htm.

[52] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1793 (codified at 50 U.S.C. §§ 1801 to 1811 (2014)).

> worker. And their co-worker says, "Oh, hey, that's great. Send that to Bill down the way," and then Bill sends it to George, George sends it to Tom, and sooner or later this person's whole life has been seen by all of these other people. The analysts don't discuss such things in the NSA cafeterias, but back in the office anything goes, more or less. You're in a vaulted space. Everybody has sort of similar clearances, everybody knows everybody. It's a small world. It's never reported, because the auditing of these systems is incredibly weak. The fact that records of your intimate moments have been taken from your private communication stream, from the intended recipient, and given to the government, without any specific authorisation, without any specific need, is itself a violation of your rights. [When asked how often do such things happen?] . . . I'd say probably every two months. It's routine enough. These are seen as sort of the fringe benefits of surveillance positions.[53]

Everyone would agree that NSA analysts should not be opening private email attachments that contain naked photos (or any non-foreign intelligence related material for that matter) and sending them to their colleagues. This is illegal and there should be repercussions. But was exposure of childish behavior by a few analysts of such significance to outweigh the damage done to our nation's security due to Snowden's disclosures?

Other reasons why Snowden made such disclosures include: (1) disgust over CIA operatives who would get targets drunk enough to land in jail and then bail them out in order to recruit an asset,[54] (2) Clapper lying in a congressional

---

[53] Alan Rusbridger & Ewan Macaskill, *I, Spy: Edward Snowden in Exile,* THE GUARDIAN, July 19, 2014, http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-interview-rusbridger-macaskill.

[54] James Bamford, *The Most Wanted Man in the World*, WIRED, Aug. 13, 2014, http://www.wired.com/2014/08/edward-snowden/.

hearing about whether the NSA collects data on Americans,[55] (3) military and CIA drones and targeted killings,[56] (4) outrage over the NSA's "ability to map the movement of everyone in a city by monitoring their MAC address, a unique identifier emitted by every cell phone, computer, and other electronic device,"[57] (5) NSA's access to email and other Internet traffic from Syria during the civil war,[58] (6) the NSA's building of a Massive Data Repository where "billions of phone calls, faxes, emails, computer-to-computer data transfers, and text messages from around the world [would] flow through the MDR every hour,"[59] and (7) the NSA's access to virtually all private communications coming in from overseas to people in the US in order to "identify these malicious traffic flows and respond to them."[60]

Again, the resounding concern is collection, and the fact that the public is not told about the mass collection. As mentioned, some of Snowden's complaints had nothing to do with bulk collection. Snowden did have a list of individual government employees whose actions merited administrative action and reprimand, but their specific activity did not undermine the legality or wisdom of the programs which Snowden was actually railing against. Snowden has certainly been successful at opening the dialogue as to bulk collection – as everyone is now discussing collection, how to reform or eliminate section 215, and how to move collection from government's hands to a third party.[61]

---

[55] At a congressional hearing on March 12, 2014, Senator Ron Wyden asked Director of National Intelligence James Clapper, "Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?" Clapper responded, "No sir . . . not wittingly." Fred Kaplan, *Fire James Clapper*, SLATE, June 11, 2013, http://www.slate.com/articles/news_and_politics/war_stories/2013/06/fire_dni_james_clapper_he_lied_to_congress_about_nsa_surveillance.html.

[56] Bamford, *supra* note 54.

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] Would a third party's (telecommunications company) employees perform better than government employees and abuse their power much less than government employees that undergo background

Transparency is important to a certain degree. It keeps the government honest and it ensures the public can keep tabs on the checks and balances that are put in place to ensure abuse does not occur. But too much transparency defeats the very purpose of clandestine intelligence operations in the first place, i.e., to protect the American public and keep the bad guys in the dark as to our intentions and capabilities. The general public has already been informed as to the purpose and mission of the NSA, plus a vague description of NSA collection platforms and capabilities is readily available. Once you delve into the details such as specific methods and sources, and the identities of certain targets, then this information becomes sensitive and classified, and as such, should be available to only those who are trusted and have a legitimate need to know. It may be advisable to have an open discussion on collection but there is no need to go into details that are classified, since such disclosures could cause harm to national security. Whistleblowers certainly need to step forward to discuss abuse within the system, especially when these failures are not being addressed by oversight committees within or outside the IC agencies. Certainly, on an individual level, when government analysts are caught monitoring calls and opening attachments that are not relevant to an authorized investigation, these people need to be brought to the attention of that agency's internal security team. However, there are multiple administrative layers of authority, policy review officials and security personnel available to anyone concerned who earnestly wants to report wrong doing or illegal activity.

One concern raised by Snowden is the allegation that the NSA "has been gathering records of online sexual activity and evidence of visits to pornographic websites as part of a proposed plan to harm the reputations of those whom the agency believes are radicalizing others [to become devoted to the jihadist cause] through incendiary speeches."[62] The six

---

checks and significant vetting before being granted top secret clearances?

[62] Glenn Greenwald, Ryan Grim, & Ryan Gallagher, *Top Secret Document Reveals NSA Spied on Porn Habits as Part of Plan to Discredit 'Radicalizers'*, HUFF. POST, Nov. 26, 2013,

"radicalizers" known to be targeted by the NSA were Muslim and all are believed to be currently residing outside the United States though one has been described as a U.S. person.[63] Snowden argued in a recent interview that this type of surveillance and individual targeting may easily find its way into U.S. politics, and these tactics could be used to spy on the pornography-viewing habits of political opponents. [64] However, there is no evidence to suggest such a giant leap has been made, and this type of slippery slope is exactly what oversight committees, supervisors, and government lawyers, need to monitor, and prevent any subsequent abuse of power.[65]

The United States Intelligence Community including the NSA collects foreign political, economic and military intelligence in order to provide U.S. policy makers with the necessary information to make the proper decisions in order to protect our national security and promote America's best interests both at home and abroad. To accomplish this goal, the IC, within certain legal limits needs to have access to every conceivable intelligence collection technique. The moral and ethical use of these tools, the potential benefits and possibility for abuse, the advisability and public acceptance for these techniques, are questions and discussions best left to the three branches of our government, and the public, to a more limited extent, to iron out.

---

http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html.

[63] *Id.*

[64] Bamford, *supra* note 54.

[65] For example, it was reported that CIA officers searched the computers of congressional staff while they prepared a Senate Intelligence Committee report on the CIA's detention and interrogation program. The CIA's inspector general investigated the matter and sent a criminal referral to the DOJ for further investigation. Mark Mazetti & Carl Hulse, *Inquiry by C.I.A. Affirms It Spied on Senate Panel*, N.Y. TIMES, July 31, 2014, http://www.nytimes.com/2014/08/01/world/senate-intelligence-commitee-cia-interrogation-report.html?_r=0. This is exactly what needs to be done when abuse of power is suspected.

IV. THE DAMAGE DONE

Chairman of the Foundation for Defense of Democracies and former Director of the CIA, James Woolsey, during a recent debate on whether Snowden was justified, described four programs which have been compromised due to the disclosures: (1) pre-Snowden, the IC had learned how to counter Chinese cyber-attacks by sending their malware back to the hackers after making some adjustments and creating problems for them; Snowden's disclosures explained how the U.S. was able to do this; (2) pre-Snowden, the IC was able to read emails and early stage drafts of emails of the Islamic State of Iraq; Snowden's disclosures allowed the terrorist group to learn of this; (3) pre-Snowden, the Defense Department had technology that allowed soldiers and CIA operatives to know whether they were being followed; post-Snowden, this technology has been shared with our adversaries; and (4) pre-Snowden, the U.S. learned how to penetrate the communication networks in some Latin American countries of some of the worst organizations and groups that are selling women, principally women into sexual slavery; post-Snowden those sex trafficking organizations now know which communication networks are compromised.[66]

Any time a government employee or unauthorized person reveals sources and methods used by law enforcement or the IC, this disclosure allows criminals, spies, and terrorists alike to minimize their risk of getting caught by taking countermeasures. When FBI Director Comey reveals that "the emergence of default encryption settings and encrypted devices and networks" will "leave law enforcement in the dark" and then names the specific companies building these devices, the concern is that criminals will use these loopholes to avoid detection.[67] The protection of sources and methods is critical to curtail illegal activity.

---

[66] Transcript of INTELLIGENCE SQUARED U.S. debate, *supra* note 43.

[67] *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? A Conversation with FBI Director James Comey*, BROOKINGS INST., Oct. 16, 2014, transcript available at http://www.brookings.edu/~/media/events/2014/10/16%20going%20dark%20technology%20privacy%20comey%20fbi/20141016_fbi_comey_transcript.pdf.

Perhaps the exposure of specific programs, sources, and methods is not the only problem, since there is now the dilemma or revelation of what was not disclosed, what does not exist, which indirectly underscores NSA limitations. In other words, if all of NSA's programs are disclosed, theoretically everything that was not revealed does not exist. NSA surveillance capabilities would be limited to the techniques exposed by Snowden and others. Criminals and terrorists alike have typically displayed signs of paranoia believing that IC capabilities approach the levels of those depicted in science fiction, and some adversaries are concerned that their every move is being watched by law enforcement. And more than likely, our sophisticated adversaries assume the government has greater surveillance powers than they actually do. The mystique of "big brother" can be a more effective weapon and deterrent than if our adversaries actually knew our true capabilities. What these disclosures have revealed is that the government has limits to what they can target, who they can target, and what they can access. As Snowden argues in his own words, "[t]he fact that people know communications can be monitored does not stop people from communicating [digitally]. Because the only choices are to accept the risk, or to not communicate at all."[68] But at least now, our adversaries know which communication service providers cooperate with the government, the specific collection techniques being used, and where the IC has focused the majority of its efforts. Our adversaries can now develop countermeasures, alternative methods of communicating with one another, and avoid or eliminate operations with identified vulnerabilities. NSA's mystique of know-all, see-all has been seriously tarnished.

Extensive damage has been done to U.S. credibility and trust issues with its foreign allies who no longer blindly trust the United States with their intelligence secrets. Our allies have reassessed the level of their cooperation on intelligence

---

[68] Bamford, *supra* note 54. "And when we're talking about things like terrorist cells, nuclear proliferators – these are organised cells. These are things an individual cannot do on their own. So if they abstain from communicating, we've already won. If we've basically talked the terrorists out of using our modern communications networks, we have benefited in terms of security – we haven't lost." *Id.*

sharing since the United States has been shown incapable of keeping secrets and even occasionally spies on its closest foreign partners. Foreign allies may be hesitant to cooperate on the next terrorism investigation. Communications service providers that were willing to cooperate with the government previously on issues dealing with national security and efforts to combat terrorism are now exposed, and may refuse to cooperate with the government in the future without being forced to do so by a court order.

V. CONCLUSION

It is not surprising Snowden revealed top secret information on NSA surveillance programs twelve years after 9/11. When the PATRIOT Act, which provided the IC and law enforcement with expansive surveillance and investigative powers, passed in 2001, the law had strong popular support. Americans feared for their safety. The government took significant legal steps to ensure they would be better able to attempt to predict and prevent another terrorist attack before it occurred, and they have been, for the most part, extremely successful in thwarting other 9/11-type attacks. Therefore, it is ironic that the IC's own success has paved the way for whistleblowers such as Snowden to gain sufficient popularity in order to reveal NSA programs under the guise of being concerned about our right to privacy. The pendulum has swung the other way, and Americans are more concerned about potentially being monitored by the government than they were immediately after 9/11. If the government had been unsuccessful in preventing attacks, the concern would be entirely different. The question would be what more can the IC do to prevent such attacks from occurring rather than the current question as to why the government is collecting so much personal data. The risk of terrorist attacks seems to be, at the very least, stabilized, and the bigger concern is our civil liberties. Due to its success, the IC is now on the defensive (for the opposite reason, i.e., intelligence failures identified post 9/11, the IC was encouraged to go on the offense). The pendulum swings in both directions.

In short, all the media hype and "24/7 surveillance state" diatribes should be taken with a grain of salt. The

moniker "big, bad government" is a misnomer although our system remains imperfect. Our leadership and government employees are for the most part decent, honest, reliable folks who are doing their jobs to the best of their ability. Some government employees are abusing their power and should be punished. When discussing government surveillance practices, there must be adequate oversight to avoid widespread, abusive practices that gradually become so pervasive that they are deemed acceptable: the habitual, standard routine that becomes self-justifying and immune to conscience and ethical scrutiny. However, full and specific disclosure when it comes to the sensitive nature of intelligence collection and its analysis is unnecessary. There are legal remedies, anonymous tip lines, and multiple avenues to report wrong doing when a whistleblower becomes concerned about "perceived" illegal activity by the government. Snowden did not pursue most of these legal remedies before disclosing classified information to the media. It is true that certain aspects of NSA's bulk collection and interception efforts may require further review and legal clarifications, but such discussions need not take place on the front page of newspapers. The recent disclosures of NSA abuse as "perceived" by Snowden do not come close to the pervasive abuses described by the Church Committee in the seventies.

Despite Snowden's pleas for an open-source community free from monitoring, the Internet is not and will not be free from surveillance regardless if the NSA participates or not. It is naive to think otherwise. The government needs to collect and analyze intelligence information in order to arrive at the best domestic, foreign, economic, military, law enforcement, or political decisions possible, and that includes policy decisions on the fight against terrorism.

In one interview, Snowden makes reference to the German Stasi that conducted "mass, indiscriminate spying campaigns"[69] in communist-dominated East Germany where the secret police collected information on roughly one quarter of the population.[70] The NSA is not the Stasi of East Germany

---

[69] Rusbridger & Macaskill, *supra* note 48.

[70] Julia Angwin, *You Know Who Else Collected Metadata? The Stasi.*, PROPUBLICA, Feb. 11, 2014,

– the NSA is not conducting mass, indiscriminate spying campaigns hoping to catch anti-government protestors in incriminating positions in order to lock them away and eliminate any and all dissent. Stasi-like dossiers are not being created on individuals who vote a certain way or oppose government policies. NSA does not monitor U.S. citizens to identify their daily activities, what errands they run, what websites they are viewing, and how their children are doing in school. What NSA does do is collect positive intelligence information, foreign intelligence information which is collected and analysed under legal parameters. These collection efforts are meant to protect U.S. citizens from future terrorist attacks and future cyber-attacks. Under section 702, targeting and minimization procedures are in place, and FISA warrants are required when the NSA wants to target U.S. citizens suspected of being agents of a foreign power.

It is not the government surveillance programs we should be overly concerned about. Public discussion and congressional and internal oversight committees keep those necessary but controversial programs under control and within legal parameters. It is the few isolated cases of individuals within the government who abuse their power and betray the American people who are of major concern, e.g., those who abuse their power and violate sections 215, 702 and FISA laws. Those are the illegalities that should be brought to light, not our government's specific sources, methods, capabilities, and successes that our enemies desperately want revealed.

---

http://www.propublica.org/article/how-the-stasi-spied-on-social-networks.

LINCOLN MEMORIAL UNIVERSITY
LAW REVIEW

VOLUME 3 FALL 2015

DAMMING THE LEAKS:
BALANCING NATIONAL SECURITY, WHISTLEBLOWING AND THE PUBLIC INTEREST

Jason Zenor[1]

In the last few years we have had a number of infamous national security leaks and prosecutions. Many have argued that these people have done a great service for our nation by revealing the wrongdoings of the defense agencies. However, the law is quite clear- those national security employees who leak classified information are subject to lengthy prison sentences or in some cases, even execution as a traitor. In response to the draconian national security laws, this article proposes a new policy which fosters the free flow of information. First, the article outlines the recent history of national security leaks and the government response to the perpetrators. Next, the article outlines the information policy of the defense industry including the document classification system, the Freedom of Information Act (FOIA), whistleblower laws and the Espionage Act. Finally, the article outlines a new policy that will advance government transparency by promoting whistleblowing that serves the public interest, while balancing it with government efficiency

[1] Assistant Professor, School of Communication, Media and the Arts, State University of New York-Oswego.

by encouraging proper channels of dissemination that actually respond to exposures of government mismanagement.

"The guarding of military and diplomatic secrets at the expense of informed representative government provides no real security for our Republic."
Justice Hugo Black[2]

"The oath of allegiance is not an oath of secrecy [but rather] an oath to the Constitution."
Edward Snowden[3]

I. INTRODUCTION

In today's digital media landscape, it is becoming more difficult to adequately balance the people's need to access information with the government's need to operate with some semblance of secrecy. U.S. legal precedent, such as *The Pentagon Papers*[4] and *Bartnicki*,[5] makes it nearly impossible for the government to punish or restrain journalists' ability to reveal lawfully obtained truthful information. Additionally, the mainstreaming of "new media"[6] has dissolved any clear

---

[2] New York Times Co. v. United States, 403 U.S. 713, 719 (1971) (Black, J., concurring).

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

[4] New York Times Co. v. United States (The Pentagon Papers), 403 U.S. 713 (1971) (holding that the Government did not show a compelling interest to restrain the publication of contents of a top-secret study that analyzed the United States' military involvement in the Vietnam War).

[5] Bartnicki v. Vopper, 532 U.S. 514 (2001).

[6] In 2009, 44% of Americans were getting their news from online or other mobile devices. 58% of Americans got their news from television, 34% from radio, and 31% from newspapers. *See generally*

definition of "journalist" and "journalism."[7] Thus, the principles that the nation seeks to protect- transparency and accountability, as well as public safety and efficient government- are being challenged, as it is uncertain who is working to inform the public and who is working to harm the status quo.[8]

When the government acts illegally or there is gross mismanagement, it is fairly easy to defend the need to expose such transgressions. Traditional media outlets do expose illegal government actions. For example, during the last decade's War on Terror, traditional media sources have revealed CIA torture of enemy combatants,[9] the existence of

---

Americans Spending More Time Following the News, PEW RES. CENTER, Sept. 12, 2010, http://people-press.org/2010/09/12/americans-spending-more-time-following-the-news/.

[7] *See* Laura Durity, *Shielding Journalist-"Bloggers": The Need to Protect Newsgathering Despite the Distribution Medium*, DUKE L. & TECH. REV., Apr. 7, 2006, at 11 (arguing that attempts at federal shield law too narrowly defined 'journalist' in the digital age).

[8] New York Times Editor Bill Keller has called WikiLeaks "a secretive cadre of anti-secrecy vigilantes." Bill Keller, *Dealing with Assange and the WikiLeaks Secrets*, N.Y. TIMES, Jan. 26, 2011, http://www.nytimes.com/2011/01/30/magazine/30Wikileaks-t.html?_r=1&adxnnl=1&adxnnlx=1301544720-v+nf9IYPS5RuUCMfTb6Aeg. More vitriolic is Conservative Pundit and Tea Party Spokesperson, Glenn Beck, who has described WikiLeaks as part of an international cabal determined to create a new world order, stating:

> What I'm talking to you about is what al Qaeda is calling "operation hemorrhage" for their part. What I have called the perfect storm, where like-minded people, people who want to destroy the republic, seize an opportunity. And the window for opportunity for anarchy and chaos on this planet, to overthrow our system here and the systems abroad is now.

Glenn Beck, *WikiLeaks Questions*, FOX NEWS, Nov. 30, 2010, http://www.foxnews.com/story/2010/11/30/glenn-beck-wikileaks-questions.html.

[9] *See, e.g.*, *Exposing the Truth of Abu Ghraib* (CBS television broadcast Dec. 10, 2006), *available at* http://www.cbsnews.com/news/exposing-the-truth-of-abu-ghraib/.

secret international prisons administered by the CIA referred to as 'black sites,'[10] and the Bush Administration's secret wiretapping and NSA surveillance programs.[11] But when it comes to shining light on the actions of our national security and defense agencies, it is not enterprising journalists who 'discover' secrets; it is employees within the agencies who decide to inform the public of the actions which they believe to be harmful to the nation.

The government did not want these transgressions revealed to the public. But no criminal charges were brought against the respective news outlets for these revelations[12] because traditional media outlets exist in a legal framework that protects journalists.[13] However, the legal framework does

---

[10] *See* Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, WASH. POST, Nov. 2, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/11/01/AR2005110101644.html. Prior to this *Washington Post* article, these sites were only known to "a handful of officials in the United States and, usually, only to the president and a few top intelligence officers in each host country." *Id.*

[11] *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html. The government argued that publication of the story would alert the terrorists that they were being watched. *Id.*

[12] To have done so would certainly have been politically unpopular, but it is possible that criminal charges would have held up in court. "Undoubtedly Congress has the power to enact specific and appropriate criminal laws to protect government property and preserve government secrets." New York Times Co., 403 U.S. at 730 (Stewart, J., concurring); *see also* Walter Pincus, *Prosecution of Journalists Is Possible in NSA Leaks*, WASH. POST, May 22, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/05/21/AR2006052100348.html.

[13] Journalists are protected by an exception under the Espionage Act and by case law such as *The Pentagon Papers* and *Bartnicki*. However, they are not constitutionally protected from being compelled to divulge their sources in federal court. *See* Branzburg v. Hayes, 408 U.S. 665 (1972). *Cf.* Jason Zenor, *Shielding Acts of Journalism: Open Leak Sites, National Security and the Free Flow of Information*, 39 NOVA L. REV. 365 (2015) (arguing for a statutory protection of journalists

not protect the sources of this information, thus the government zealously pursues the leakers.[14]

In 2013, Edward Snowden gained infamy after he fled the country and leaked classified information pertaining to an NSA surveillance program.[15] Some argue that Snowden is a patriot and hero.[16] He opened our eyes- though it was widely suspected, most Americans did not realize the span of government surveillance that was happening and what was allowed by the PATRIOT Act.[17] The leaks also revealed illegal surveillance of foreign leaders.[18] He exposed the actions of the government which are not supported by the Constitution.

Yet, others argue that Snowden's leaks have severely harmed the U.S. government's interests.[19] They made the government's enemies, specifically terrorist groups, aware of how the U.S. intelligence entities operate. They have soured relationships between U.S. and foreign governments, especially those in which it was revealed that the U.S. had spied on them. Furthermore, foreign governments and private companies working with the U.S. government may be hesitant to share information for fear it will be exposed. Ultimately, the government is fearful that every secret is now fair game and a government cannot function in this way.

---

who disseminate leaked national security information that serves the public interest).

[14] 18 U.S.C. § 793 (2012).

[15] Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 6, 2013, http://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.

[16] *See, e.g.*, Douglas Rushkoff, *Edward Snowden is a Hero*, CNN, June 10, 2013, http://www.cnn.com/2013/06/10/opinion/rushkoff-snowden-hero/index.html.

[17] Risen & Lichtblau, *supra* note 11.

[18] *See generally, Snowden NSA: Germany to Investigate Merkel Phone Tap*, BBC NEWS, June 4, 2014, http://www.bbc.com/news/world-europe-27695634.

[19] *See, e.g.*, Michael Hayden, *Ex-CIA Chief: What Edward Snowden Did*, CNN, July 19, 2013, http://www.cnn.com/2013/07/19/opinion/hayden-snowden-impact/index.html.

This article attempts to resolve the unease caused by national security leaks by proposing a new policy on the free flow of information in the 21st Century. This proposal attempts to balance government transparency with government efficiency. This new policy will advance transparency by promoting 'whistleblowing' on national security misconduct. It will promote government efficiency by encouraging proper channels of dissemination while guaranteeing protections that current laws do not. Part II of the article outlines the recent history of national security leaks and the government response to the perpetrators. Part III of the article outlines the information policy of the defense industry including the document classification system, FOIA, whistleblower law and the Espionage Act. Finally, Part IV of the article proposes the new policy that will advance government transparency by promoting whistleblowing that serves the public interest, while balancing it with government efficiency by encouraging proper channels of dissemination and responsive government.

II. THE WHISTLEBLOWERS

A. BRADLEY MANNING

Bradley Manning was an intelligence analyst who reviewed classified material during the Iraq War.[20] In 2010, Manning copied much of the classified material that she encountered and leaked it to WikiLeaks, an open leaks site that uses encrypted software to protect anonymity of those who leak classified information.[21] WikiLeaks published thousands of documents including the "Afghan War Diary,"[22]

---

[20] *Profile: Private First Class Manning*, BBC NEWS, Apr. 23, 2014, http://www.bbc.com/news/world-us-canada-11874276.

[21] Paul Courson & Matt Smith, *WikiLeaks Source Manning Gets 35 Years, Will Seek Pardon*, CNN, Aug. 22, 2013, http://www.cnn.com/2013/08/21/us/bradley-manning-sentencing/.

[22] This consisted of over 750,000 pages of never-before-released documents relating to the war in Afghanistan. *See* Alastair Dant & David Leigh, *Afghanistan War Logs: Our Selection of Significant Incidents*, THE GUARDIAN, July 25, 2010,

"The Iraq War Logs,"[23] and State Department documents known as "Cablegate."[24] They also released a video titled "Collateral Murder" which showed gun-sight footage of a 2007 airstrike in Baghdad that killed a Reuters reporter and innocent civilians including children.[25]

Manning had confided in a friend, Adrian Lamo, that she had leaked the information.[26] Lamo then notified the U.S.

---

http://www.guardian.co.uk/world/datablog/interactive/2010/jul/25/afghanistan-war-logs-events.

[23] This consisted of almost 400,000 documents relating to the war in Iraq. *See Iraq: The War Logs*, THE GUARDIAN, http://www.guardian.co.uk/world/iraq-war-logs.

[24] Julian Barnes, *What Bradley Manning Leaked*, WALL STREET J., Aug. 21, 2013, http://blogs.wsj.com/washwire/2013/08/21/what-bradley-manning-leaked/.

[25] Full footage of Collateral Murder is available at: *Collateral Murder – Wikileaks – Iraq*, YOUTUBE.COM, http://www.youtube.com/verify_age?next_url=http%3A//www.youtube.com/watch%3Fv%3D5rXPrfnU3G0. Julian Assange, WikiLeaks founder, commented on the naming of the video: "[w]e want to knock out this 'collateral damage' euphemism, and so when anyone uses it they will think, 'collateral murder.'" Greg Mitchell, *One Year Ago: How the 'Era of WikiLeaks' Began – With 'Murder'*, HUFF. POST, Mar. 28, 2011, http://www.huffingtonpost.com/greg-mitchell/one-year-ago-how-the-era_b_841376.html). The soldiers' reactions are documented on the film: "[l]ook at those dead bastards," one pilot says. "Nice," the other responds. A wounded man can be seen crawling and the pilots impatiently hope that he will try to fire at them so that, under the rules of engagement, they can shoot him again. "All you gotta do is pick up a weapon," one pilot says. A short time later a van arrives to pick up the wounded and the pilots open fire on it, wounding two children inside. "Well, it's their fault for bringing their kids into a battle," one pilot says. At another point, an American armored vehicle arrives and appears to roll over one of the dead. "I think they just drove over a body," one of the pilots says, chuckling a little. The U.S. media had initially covered the incident, but little time was spent on it. *See, e.g.*, Alissa Rubin, *2 Iraqi Journalists Killed as U.S. Forces Clash with Militias*, N.Y. TIMES, July 13, 2007, http://www.nytimes.com/2007/07/13/world/middleeast/13iraq.html.

[26] Ed Pilkington, *Adrian Lamo Tells Manning Trial About Six Days of Chats with Accused Leaker*, THE GUARDIAN, June 4, 2013,

Army of Mannings' actions.[27] Just weeks after the video was posted, the military arrested Manning and she was charged with twenty-two offenses including violations of the Espionage Act and "aiding the enemy."[28] In February 2013, Manning pled guilty to ten counts and was tried for the remaining charges.[29] In July 2013, Bradley Manning was convicted on seventeen counts and sentenced to thirty-five years in prison.[30] She is serving her sentence in maximum security at the Army's Fort Leavenworth prison in Kansas.[31]

B. EDWARD SNOWDEN

Edward Snowden worked for the CIA from 2006-2009.[32] Starting in 2009, Snowden worked as a private national security contractor with the NSA's surveillance programs.[33] In 2013, he left his contracting job and flew to Hong Kong with a plan to leak classified information about the NSA's surveillance programs to the press.[34]

---

http://www.theguardian.com/world/2013/jun/04/adrian-lamo-testifies-bradley-manning.

[27] *Id.*

[28] Conviction of "aiding the enemy" could have resulted in execution. Jim Miklaszewski & Courtney Kube, *Manning Faces New Charges, Possible Death Penalty*, NBC NEWS, Mar. 3, 2011, http://www.nbcnews.com/id/41876046/ns/us_news-security/t/manning-faces-new-charges-possible-death-penalty/#.VNhBGXIo600.

[29] *Profile: Private First Class Manning*, *supra* note 20.

[30] Manning was acquitted of aiding the enemy which may have been punishable by execution. He has the possibility of parole after another eight years. Courson & Smith, *supra* note 21.

[31] John Hanna, *Bradley Manning Prison Term Will Be Served at Fort Leavenworth,* HUFF. POST, Aug. 21, 2013, http://www.huffingtonpost.com/2013/08/21/bradley-manning-prison_n_3792135.html.

[32] John Broder & Scott Shane, *For Snowden, A Life of Ambition, Despite the Drifting*, N.Y. TIMES, June 15, 2013, http://www.nytimes.com/2013/06/16/us/for-snowden-a-life-of-ambition-despite-the-drifting.html?pagewanted=all.

[33] *Id.*

[34] *Id.* Snowden claimed that he had made several complaints to his superiors about the legality of the surveillance program, but was told to remain quiet. The U.S. government claims that there is no

The Guardian published Snowden's claims that the NSA, with the Foreign Intelligence Surveillance Court's approval, was collecting telephone records both internationally and domestically.[35] *The Guardian* released specific information on the NSA's methodologies, the operation of classified intelligence courts, and the U.S. government's relationship with foreign governments.[36] The information implicated the wrongdoing of both the U.S. and U.K. governments.[37]

Shortly after the publications, Snowden publically identified himself as the source of the leak.[38] The U.S. government charged Snowden with violating the Espionage Act by stealing and disclosing state secrets.[39] Snowden spent several weeks as a fugitive while he waited for asylum.[40] Finally, Russia granted asylum to Snowden in August of 2013, where he remains.[41]

---

evidence that Snowden ever made complaints. *See* Charlie Savage, *Snowden Says He Reported N.S.A. Surveillance Concerns Before Leaks*, N.Y. TIMES, Mar. 7, 2014, http://www.nytimes.com/2014/03/08/world/europe/snowden-says-he-reported-nsa-surveillance-concerns-before-leaks.html.

[35] *See generally,* Ewen MacAskill & Gabriel Dance, *NSA Files: Decoded*, THE GUARDIAN, Nov. 1, 2013, http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

[36] *Id.*

[37] *Id.*

[38] Barton Gellman, Aaron Blake & Greg Miller, *Edward Snowden Comes Forward as Source of NSA Leaks*, WASH. POST, June 9, 2013, http://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html.

[39] This crime carries a punishment of not more than ten years in prison. 18 U.S.C. § 798(a) (2012).

[40] Andre de Nesnera, *Snowden May Face Tough Time in Russian Asylum*, VOICE OF AMERICA (Aug. 22, 2013), http://www.voanews.com/content/snowden-may-face-rocky-road-in-russia/1734858.html.

[41] *Id.* The initial grant was for one year, but Russia then granted Snowden a three year residency. Michael Birnbaum, *Russia Grants Edward Snowden Residency for Three More Years*, WASH. POST, Aug. 7, 2014, http://www.washingtonpost.com/world/europe/russia-grants-edward-snowden-residency-for-3-more-

C. THOMAS DRAKE

Thomas Drake was an intelligence analyst who went to work for the NSA in 2001.[42] He held several jobs with the NSA, including working in the Signals Intelligence Directorate, Cryptologic Systems and Professional Health Office and in the Directorate of Engineering.[43] Drake worked on developing intelligence collection through digital networks.[44] At that time there were two main tools that the NSA was deciding between: the Trailblazer Project and the ThinThread Project.[45] Drake favored the ThinThread project because he felt it protected the privacy of U.S. citizens and was a fraction of the cost.[46] However, the NSA decided to move forward with the Trailblazer Project.[47]

Drake felt that the NSA's actions were mismanagement and waste.[48] In 2002, he decided to report it through the proper channels, including his superiors, the NSA Inspector General, the Inspector General of the Department of Defense, and the Congressional Intelligence Committees of both houses of Congress.[49] In 2004, the NSA Inspector General found that Drake's concerns were legitimate and the Trailblazer project

---

years/2014/08/07/8b257293-1c30-45fd-8464-8ed278d5341f_story.html.

[42] His first day was September 11th, 2001. Jane Mayer, *The Secret Sharer*, THE NEW YORKER, May 23, 2011, http://www.newyorker.com/magazine/2011/05/23/the-secret-sharer.

[43] Frederick Reese, *Sacrifices in Journalism and Whistleblowing: A Tribute to Truth-Tellers*, MINT PRESS, Jan. 30, 2015, http://www.mintpressnews.com/sacrifices-in-journalism-and-whistleblowing-a-tribute-to-truth-tellers/200119/.

[44] *Id*.

[45] Mayer, *supra* note 42.

[46] *Id*.

[47] *Id*.

[48] *Id*.

[49] Ellen Nakashima, *Former NSA Executive Thomas A. Drake May Pay High Price for Media Leak*, WASH. POST, July 14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/07/13/AR2010071305992.html.

was wasteful at a price-tag of over $1 billion.[50] The Department of Defense echoed those concerns in its subsequent reports.[51]

In 2006, Drake told *Baltimore Sun* reporter Siobhan Gorman about the waste happening at the NSA, including the Trailblazer program.[52] In 2007, the FBI raided Drake's home and found classified material in his possession.[53] In 2010, a grand jury in Baltimore, Maryland indicted Drake pursuant to the Espionage Act for willfully releasing national defense information,[54] as well as obstructing justice and making false statements to a federal officer.[55]

Drake was not charged with disclosing classified information.[56] Nonetheless, he faced a possible thirty-five years in prison.[57] The U.S. government claimed that the prosecution was not in retaliation to Drake's reporting of NSA waste, rather the prosecution stood on the merits of the case.[58]

---

[50] R. Jeffrey Smith, *Classified Pentagon Report Upholds Thomas Drake's Complaints About NSA*, WASH. POST, June 22, 2011, http://www.washingtonpost.com/national/national-security/classified-pentagon-report-upholds-thomas-drakes-complaints-about-nsa/2011/06/22/AG1VHTgH_story.html.

[51] *Id*.

[52] Siobhan Gorman, *Second-Ranking NSA Official Forced Out of Job by Director*, BALTIMORE SUN, May 31, 2006, http://articles.baltimoresun.com/2006-05-31/news/0605310010_1_alexander-black-spy-agency.

[53] Gabrielle Levy, *Exclusive Interview: NSA Whistleblower on What He'd Do Differently Now*, UPI, May 7, 2014, http://www.upi.com/Top_News/US/2014/05/07/Exclusive-Interview-NSA-whistleblower-on-what-hed-do-differently-now/1511399476082/.

[54] 18 U.S.C. § 793(e) (2012).

[55] 18 U.S.C. § 1001(a) (2012).

[56] *Bio: Thomas Drake*, GOVERNMENT ACCOUNTABILITY PROJECT, http://www.whistleblower.org/bio-thomas-drake (last visited Jan. 28, 2014).

[57] David Wise, *Leaks and the Law: The Story of Thomas Drake*, SMITHSONIAN MAG., Aug. 2011, http://www.smithsonianmag.com/history/leaks-and-the-law-the-story-of-thomas-drake-14796786/.

[58] 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.

Drake eventually struck a deal with the prosecution and pled guilty to a misdemeanor for misusing NSA's computer system.[59] He was sentenced to one year probation and community service.[60]

D. STEPHEN JIN-WOO KIM

Stephen Jin-Woo Kim was a private contractor that worked as a Senior Advisor in the State Department's Bureau of Verification, Compliance, and Implementation.[61] His job was to analyze North Korea's nuclear program.[62] In 2009, Kim told FOX News journalist James Rosen that North Korea was planning to test a nuclear bomb.[63] In 2010, a grand jury indicted Kim pursuant to the Espionage Act for unauthorized disclosure of defense information,[64] as well as making false statements.[65] The information that Kim disclosed was not classified, but the information was in relation to 'national defense.'[66] Kim pled guilty to disclosing national defense information and was sentenced to thirteen months in prison.[67]

---

[59] Wise, *supra* note 57.
[60] *Id.*
[61] Government's Memorandum in Aid of Sentencing at 2, United States v. Jin-Woo Kim, 2013 WL 3866545 (D.D.C. July 24, 2013), *available at* http://fas.org/sgp/jud/kim/032414-sent.pdf.
[62] *Id.*
[63] Conor Friedersdorf, *Did James Rosen's Story on North Korea Do Any Harm?*, THE ATLANTIC, May 23, 2013, http://www.theatlantic.com/politics/archive/2013/05/did-james-rosens-story-on-north-korea-do-any-harm/276152/.
[64] 18 U.S.C. § 793(d).
[65] 18 U.S.C. § 1001(a)(2).
[66] Mark Hosenball, *Justice Department Indicts Contractor in Alleged Leak*, NEWSWEEK, Aug. 27, 2010, http://www.newsweek.com/justice-department-indicts-contractor-alleged-leak-217186.
[67] Josh Gerstein, *Contractor Pleads Guilty in Leak Case*, POLITICO, Feb. 7, 2014, http://www.politico.com/story/2014/02/stephen-kim-james-risen-state-department-fox-news-103265.

E. JEFFREY STERLING

Sterling began working as an officer for the CIA in 1993.[68] In 2000, Sterling filed a complaint with the CIA's Equal Employment Office alleging racial discrimination.[69] In 2001, Sterling was placed on administrative leave, and his classified information privileges were revoked.[70] In 2002, the CIA terminated him.[71] Sterling's subsequent lawsuit against the CIA was dismissed because the trial would have disclosed classified information.[72] In 2005, the Fourth Circuit Court of Appeals upheld the case's dismissal.[73]

In 2010, the U.S. government indicted Sterling for violating the Espionage Act with his unauthorized disclosure of the national defense information.[74] The government discovered emails and telephone communication between Sterling and *The New York Times* reporter, James Risen.[75] The U.S. government claimed that Sterling detailed the CIA's secret plot to disrupt Iran's nuclear program by giving the

---

[68] Matt Apuzzo, *C.I.A. Officer is Found Guilty in Leak Tied to Times Reporter*, N.Y. TIMES, Jan. 26, 2015, http://www.nytimes.com/2015/01/27/us/politics/cia-officer-in-leak-case-jeffrey-sterling-is-convicted-of-espionage.html?_r=0.

[69] *Id*.

[70] *Former CIA Officer Convicted of Violating Espionage Act*, SKY VALLEY NEWS, Jan. 28, 2015, http://www.skyvalleychronicle.com/FEATURE-NEWS/FORMER-CIA-OFFICER-CONVICTED-OF-VIOLATING-ESPIONAGE-ACT-br-i-And-here-s-the-back-story-much-of-the-news-media-did-not-report-i-2002227.

[71] *Id*.

[72] Josh Gerstein, *Ex-CIA Officer Found Guilty in Leak Trial*, POLITICO, Jan. 26, 2015, http://www.politico.com/story/2015/01/jeffrey-sterling-convicted-cia-leak-trial-114605.html.

[73] *See* Sterling v. Tenet, 416 F.3d 338 (4th Cir. 2005); *see also* Warren Richey, *Former Covert CIA Agent Charged with Leaking Secrets to Newspaper*, CHRISTIAN SCI. MONITOR, Jan. 6, 2011, http://www.csmonitor.com/USA/Justice/2011/0106/Former-covert-CIA-agent-charged-with-leaking-secrets-to-newspaper.

[74] The indictment also charged mail fraud and obstruction of justice. Apuzzo, *supra* note 68.

[75] *Id*.

foreign government misinformation.[76] Risen wrote about the mission in his book and painted it as a mismanaged and potentially dangerous campaign that may have aided Iran's nuclear program.[77]

Sterling pled not guilty to all counts.[78] There was no direct proof that Sterling had given this information to Risen.[79] In fact, Sterling had gone to the U.S. Senate in 2003 to report the program.[80] His attorneys argued that Risen could have pieced together the information from leaks on Capitol Hill.[81] Despite the lack of solid evidence, in January 2015, Sterling was convicted. In May 2015 he was sentenced to forty-two months, much less than had been anticipated.[82]

III. LEGAL BACKGROUND

A. FIRST AMENDMENT AND FREE FLOW OF INFORMATION

The paramount concern of the First Amendment is to protect the free flow of information to the people concerning issues of public interest.[83] As Justice's Black and Douglas explained in concurring opinions in *The Pentagon Papers*,

---

[76] *Id*.

[77] *See generally*, JAMES RISEN, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION (2006).

[78] *See* Apuzzo, *supra* note 68.

[79] *Id*.

[80] *Id*.

[81] Sterling claimed that he only discussed his discrimination suit against the CIA with Risen. *Id*.

[82] Matt Apuzzo, *Ex-C.I.A. Officer Sentenced in Leak Case Tied to Times Reporter*, May 11, 2015, http://www.nytimes.com/2015/05/12/us/ex-cia-officer-sentenced-in-leak-case-tied-to-times-reporter.html.

[83] *See* Garrison v. Louisiana, 379 U.S. 64, 77, 85 (1964). As Justice Breyer argued in *Garcetti*: "Government administration typically involves matters of public concern. Why else would government be involved? And 'public issues,' indeed, matters of 'unusual importance,' are often daily bread-and-butter concerns for the police, the intelligence agencies, the military, and many whose jobs involve protecting the public's health, safety, and the environment." Garcetti v. Ceballos, 547 U.S. 410, 448 (2006) (Breyer, J., dissenting).

"[s]ecrecy in government is fundamentally anti-democratic."[84] When our government shrouds itself in secrecy, it "provides no real security for our Republic."[85] Accordingly, it is "only a free and unrestrained press [that] can effectively expose deception in government,"[86] but, "[a] free press cannot be made to rely solely upon the sufferance of government to supply it with information."[87] Instead, it is government employees speaking out against their employers who are often in the best position to expose deception in government.[88] Consequently, public debate has much to gain when government employees speak.[89]

B. ACCESS TO INFORMATION

1. FREEDOM OF INFORMATION ACT

The federal Freedom of Information Act (FOIA) was passed in 1966.[90] Prior to FOIA, the only two public information laws were the Administrative Procedures Act of

---

[84] New York Times Co. v. United States, 403 U.S. 713, 724 (1971) (Douglas, J., concurring).
[85] *Id.* at 719 (Black, J., concurring).
[86] *Id.* at 717 (Black, J., concurring).
[87] Smith v. Daily Mail Publ'g, 443 U.S. 97, 104 (1979) (holding that newspapers could not be punished for publishing the name of a juvenile rape victim discovered from listening to police radio signals).
[88] *See* Pickering v. Bd. of Educ., 391 U.S. 563 (1968) (holding that government employee speech could not be abridged unless the government could show that the employee was not speaking on a matter of public concern and it disrupted government administration).
[89] *Id*.
[90] *See* Martin E. Halstuk, *When Secrecy Trumps Transparency: Why the Open Government Act of 2007 Falls Short*, 16 COMMLAW CONSPECTUS 427 (2008) (detailing the history of FOIA); *see also* Martin Halstuk, *The Freedom of Information Act 1966-2006: A Retrospective on the Rise of Privacy Protection over the Public Interest in What the Government's up to*, 11 COMM. L. & POL'Y 511 (2006) (detailing the evolution of privacy exemptions in FOIA).

1946[91] and the Housekeeping Statute of 1789.[92] Both Acts gave the executive branch unlimited discretion as to what information it could keep secret.[93] FOIA, on the other hand, amended the APA to add a presumption of openness for all federal documents.[94] But FOIA did provide nine exemptions, including one for national security.[95] Other exemptions included trade secrets,[96] personal privacy rights,[97] internal practices,[98] and ongoing law enforcement proceedings.[99] FOIA has eliminated much of the government's preference for secrecy in order to protect political embarrassment and concordantly, courts have construed the exemptions narrowly.[100]

In 1974, after Watergate, Congress amended the FOIA because of perceived abuse with the national security

---

[91] Administrative Procedure Act § 3, Pub. L. No. 79-404, 60 Stat. 237, 238 (1946).

[92] Act of Sept. 15, 1789, ch. 14, 1 Stat. 68 (codified as amended at 5 U.S.C. § 301 (2006)).

[93] *See* Halstuk, *supra* note 90.

[94] *See, e.g.*, John Doe Agency v. John Doe Corp., 493 U.S. 146, 152 (1989).

[95] 5 U.S.C. § 552(b)(1)(A) (2012) ("This section does not apply to matters that are specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy[.]").

[96] 5 U.S.C. §552(b)(4) ("This section does not apply to matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential[.]").

[97] 5 U.S.C. § 552(b)(6) ("This section does not apply to matters that are personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy[.]"); *See also* S. Rep. No. 89-813, at 38 (1965) ("At the same time that a broad philosophy of 'freedom of information' is enacted into law, it is necessary to protect certain equally important rights of privacy . . . such as medical and personnel files.").

[98] 5 U.S.C. § 552(b)(2), (5); *See also* S. Rep. No 89-813, at 44 (1965) (Exception 5 recognized that the "[g]overnment would be greatly hampered if, with respect to legal and policy matters, all Government agencies were prematurely forced to 'operate in a fishbowl.'").

[99] 5 U.S.C. § 552(b)(7).

[100] *See, e.g.*, Dep't of Air Force v. Rose, 425 U.S. 352, 361 (1976) (granting FOIA request for Air Force Academy Honor Code).

exemption.[101] Congress also amended the law enforcement exemption to require that the government show the requested record was compiled for law enforcement and that publication would result in an enumerated harm.[102] But, in 1986, the national security and law enforcement exemption were expanded to include terrorism.[103] It also exempted matters that are "specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and are in fact properly classified pursuant to such Executive Order."[104] Furthermore, in FOIA cases dealing with national security exemptions, courts continue to give great deference to the executive branch defining what constitutes potential harms from releasing documents.[105]

2. GOVERNMENT DOCUMENT CLASSIFICATION SYSTEM

At the federal level, documents can be classified as "top secret," "secret," or "confidential."[106] The last two overhauls of the government document classification system came in 1995[107] and 2003,[108] during the Clinton and Bush

---

[101] *See* Halstuk, *supra* note 90.
[102] *Id.*
[103] *See* James Goldston, Jennifer Granholm & Robert Robinson, *A Nation Less Secured: Diminished Public Access to Information*, 21 HARV. C.R.-C.L. L. REV 409 (1986) (reviewing 1986 amendments to FOIA).
[104] 5 U.S.C. § 552(b)(1).
[105] It is "well-established that the judiciary owes some measure of deference to the executive in cases implicating national security, a uniquely executive purview." Ctr. for Nat'l Security Studies v. Dep't of Justice, 331 F.3d 918, 926-27 (D.C. Cir. 2003) (denying FOIA request for name of detainees). *Cf.* Nathan Slegers, *De Novo Review Under The Freedom of Information Act: The Case Against Judicial Deference to Agency Decisions to Withhold Information*, 43 SAN DIEGO L. REV. 209 (2006).
[106] *See* David McGinty, *The Statutory and Executive Development of the National Security Exemption to Disclosure Under the Freedom of Information Act: Past and Present*, 32 N. KY. L. REV. 67 (2005).
[107] *Classified National Security Information* (Clinton Order), Exec. Order No. 12,958, 60 Fed. Reg. 19,825, 19,843 (Apr. 17, 1995). Prior to FDR Administration establishing a classification system, each agency had

Administrations respectively. Under the Clinton Order, a document must have an articulable impact on national security in order to be classified.[109] National security was defined as "national defense or foreign relations of the United States."[110] The Clinton Order established the Interagency Security Classification Appeals Panel (ISCAP) that reviews employee and public (non-FOIA) challenges to the classification of documents.[111] The President appoints the members of ISCAP and is made of senior level members of the Department of Defense, Department of State, Department of Justice, and National Archives.[112]

In 2003, the Bush Order amended the 1995 order.[113] First, it removed a clause that stated information "shall not be classified" whenever there "is significant doubt about the need

---

full discretion to classify documents without requiring justification. *See* Exec. Order No. 8381. 5 Fed. Reg. 1147 (Mar. 22, 1940).

[108] Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 25, 2003) *reprinted as amended* in 50 U.S.C. § 435 (2006).

[109] Prior to the Clinton Order, there was a category that protected "confidential sources" and an ambiguous "catchall category." *See* McGinty, *supra* note 106.

[110] In order to be labeled confidential, there has to be identifiable damage if the document were to be released. Information that can be classified includes:

> "military plans, weapons systems, or operations"; "foreign government information"; "intelligence activities (including special activities), intelligence sources or methods, or cryptology"; "scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism"; "United States Government programs for safeguarding nuclear materials or facilities"; "vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism"; or "weapons of mass destruction."

Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 25, 2003).

[111] *See Classified National Security Information* (Clinton Order), *supra* note 107.

[112] *Id.*

[113] Exec. Order No. 13,292, *supra* note 108.

to classify" it.[114] The Bush Order also omitted a requirement to classify information at the lower of two possible classification levels when there is uncertainty as to which level is appropriate.[115] The Bush Order also added that "[t]he unauthorized disclosure of foreign government information is presumed to cause damage to the national security."[116] Finally, the 2003 order allows for the reclassification of previously declassified, public documents. [117]

In 2009, the Obama Administration executed its own order to amend the classification system. The new system has a presumption against classification.[118] Also, employees are expected to voice objections to the ISCAP when they disagree with classifications in good faith.[119] But, agencies have discretion to classify any information that may hurt national security−though this is not defined.[120] National Security agency heads can also delay the ISCAP declassification of documents by seeking an appeal to the President.[121]

---

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] *Id. See* Jane Kirtley, *Transparency and Accountability in a Time of Terror: The Bush Administration's Assault on the Freedom of Information*, 11 COMM. L. & POL'Y 479 (2006) (reviewing how the Bush Administration's changes to classification systems affected free flow of information).

[118] Exec. Order No. 13,526 § 1.1(b), 75 Fed. Reg. 707 (Dec. 29, 2009).

[119] *Id.* at § 1.8.

[120] *Id.* at § 1.2. *Cf.* Reducing Over-Classification Act, H.R. 553, 111th Cong. (2010). The purpose of the act is to "prevent federal departments and agencies from unnecessarily classifying information or classifying information at a higher and more restricted level than is warranted, and by doing so to promote information sharing across departments and agencies and with State, local, tribal and private sector counterparts, as appropriate." *Id*. For a discussion on the classification system in the United States, *see* Wendy Keefer, *Protection of Information to Preserve National Security: Is WikiLeaks Really the Issue?*, 5 CHARLESTON L. REV. 457 (2011).

[121] *Id.* at § 3. Between 1996-2008, ISCAP voted to declassify (whole or in-part) 495 of 796 documents (64%). Steven Aftergood, *Reducing Government Secrecy: Finding What Works*, 27 YALE L. & POL'Y REV. 399, 407 (2009). Despite the ISCAP's acceptance of transparency, there is plenty of evidence that executive agencies have become more secret after 9/11, often invoking the mosaic theory that even documents

C. STATUTORY PROTECTIONS AND PUNISHMENTS

1. FEDERAL WHISTLEBLOWER LAWS

Federal employees are protected by a patchwork of whistleblower protections.[122] These laws include Whistleblower Act of 1989,[123] which protects civilian employees from wrongful dismissal, and the No FEAR Act,[124] which makes agencies directly and financially responsible for illegal retaliation. The Department of Labor houses the Office of the Whistleblower Protection Program that "administers the whistleblower protection provisions of more than twenty whistleblower protection statutes" for civilian employees.[125] Members of the U.S. military are protected by the Military

---

that, on their own, do not concern national security are connected somehow to national security interests, thus, must be classified. *See, e.g.*, David Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L. J. 628 (2005).

[122] *See* Sarah Wood Borak, *The Legacy of "Deep Throat": The Disclosure Process of the Whistleblower Protection Act Amendments of 1994 and the No FEAR Act of 2002*, 59 U. MIAMI L. REV. 617 (2005) (documenting the history of federal whistleblower statutes). Congress passed the first Whistleblower statutes in 1778. The law protected soldiers who reported inhumane treatment of POWs. Stephen M. Kohn, *The Whistle-Blowers of 1777*, N.Y. TIMES, June 12, 2011, http://www.nytimes.com/2011/06/13/opinion/13kohn.html.

[123] Pub. L. No. 101-12, 103 Stat. 16 (1989) (codified as amended 5 U.S.C. § 2302 (2012)).

[124] Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act), Pub. L. No. 107-74, § 104, 116 Stat. 566 (2002).

[125] Federal employees can "report violations of workplace safety and health, airline, commercial motor carrier, consumer product, environmental, financial reform, food safety, health insurance reform, motor vehicle safety, nuclear, pipeline, public transportation agency, railroad, maritime, and securities laws." The employees are protected from retaliation in the form of "blacklisting, demoting, denying overtime or promotion, disciplining, denial of benefits, failure to hire or rehire, intimidation, making threats, reassignment affecting prospects for promotion, or reducing pay or hours[.]" DEPARTMENT OF LABOR, THE WHISTLEBLOWER PROTECTION PROGRAMS, www.whistleblowers.gov (last visited Jan. 22, 2015).

Whistleblower Protection Act.[126] This Act protects the military members' ability to report a violation of the law to members of Congress, Inspector Generals, chains of command, or other law enforcement.[127]

In 2006, the U.S. Supreme Court decided *Garcetti v. Ceballos*.[128] The case limited the free speech rights of government employees by not protecting speech that was conducted within the official job duties.[129] The U.S. House of Representatives responded by proposing a bill titled the Whistleblower Protection Enhancement Act of 2007.[130] The bill would have expanded the protections afforded to federal employees who disclosed government waste, fraud and abuse.[131] The Act also granted access to jury trials[132] for government employees who had been retaliated against. The

---

[126] *See* 10 U.S.C. § 1034 (2012).

[127] Military members can report "sexual harassment, unlawful discrimination, gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial or specific danger to public health or safety." UNITED STATES COAST GUARD, THE MILITARY WHISTLEBLOWER PROTECTION ACT, http://www.uscg.mil/legal/MilitaryWhistlerBlowerProtectionAct.asp (last visited Jan. 22, 2015).

[128] 547 U.S. 410 (2006). With the nebulous nature of job descriptions and the perpetuity of the workday due to advances in technology, it is arguable that a public employee is always working and can never speak without representing his or her employer. *See generally* Robert Drechsel, *The Declining First Amendment Rights of Government News Sources: How Garcetti v. Ceballos Threatens the Flow of Newsworthy Information*, 16 COMM. L & POL'Y 129 (2011) (arguing that the *Garcetti* prong has greatly curtailed public employee speech and the free flow of information).

[129] 547 U.S. at 423.

[130] H.R. 985, 110th Cong. (2007).

[131] *Id.*

[132] Over the last seventeen years of whistleblower cases, the federal courts have sided with the government 210 times while siding with whistleblowers only three times. *See* Anniston Star Editorial Board, *Holding up Progress, Senate's Shameful Little Secret*, ANNISTON STAR, Mar. 14, 2011, http://annistonstar.uber.matchbin.net/pages/full_story/push?article-Holding+up+progress-+Senate-s+shameful+little+secret%20&id=12326421.

House passed the bill by a margin of 331-94.[133] The Senate then passed its own whistleblower bill.[134] But, it contained fewer protections with no access to jury trials.[135] As a result, the two houses were unable to negotiate a compromise and the bill failed.[136]

In 2009, the Senate proposed another Whistleblower Protection Enhancement Act. This bill would have provided for jury trials for federal employees and even protected employees in national security positions.[137] However, in 2010 after WikiLeaks revealed hundreds of leaked documents, Congress began to strip much of the legislation's protections, including those for national security workers.[138] Finally, in 2012 the Whistleblower Protection Enhancement Act was finally passed.[139]

Whistleblower law provides little protection for those who leak national security information. Congress recognized this and passed the Intelligence Community Whistleblower Protection Act of 1998.[140] This Act protected all employees and contractors of national security agencies who disclosed maters of "urgent concern" such as violation of the law, false statement to Congress, or retaliation against protected whistleblowers.[141] However, whistleblowers could not make

---

[133] *Id.*

[134] Federal Employee Protection of Disclosures Act, S. 274, 110th Cong. (2007).

[135] *Id.*

[136] *See Holding up Progress, Senate's Shameful Little Secret*, *supra* note 132.

[137] The Senate added the national security clause after two Department of Homeland Security officials lost their jobs after alleging agency abuses. *See* Alan Maimon, *WikiLeaks Furor Causes Defeat of Rights Bill with Las Vegas Ties*, LAS VEGAS J. REV., Mar. 30, 2011, http://www.lvrj.com/news/-wikileaks-furor-causes-defeat-of-rights-bill-with-lv-ties-114920289.html.

[138] *See* Project on Government Oversight, *How a Red Herring About WikiLeaks Killed Whistleblower Protections*, HUFF. POST, Jan. 7, 2011, http://www.huffingtonpost.com/project-on-government-oversight/how-a-red-herring-about-w_b_805915.html.

[139] Pub.L. No. 112–199, § 108(a), 126 Stat. 1468 (codified as amended at 5 U.S.C. § 7703(b)(1)).

[140] Pub.L. No. 105–272, Title VII, 112 Stat. 2396 (1998) (codified as amended at 5 U.S.C. § 2302).

[141] 50 U.S.C. § 3024 (2013).

disclosures directly to Congress. They had to make disclosures to the respective agency's Inspector General who then must inform the agency head.[142] Furthermore, the Inspector General's decisions are not subject to judicial review.[143] Finally, agencies are open to remove security clearance, as courts have held that this is not a form of retaliation that is subject to review.[144]

In 2012, the Obama Administration published Presidential Policy Directive 19.[145] The directive extends some whistleblower protection to national security employees. Such employees cannot suffer retaliation for good faith reports of waste or fraud to his or her superiors, Inspector Generals or the Director of National Intelligence.[146] Employees can appeal decisions of their superiors to a three-person panel made up of Inspector Generals, but the panel's decision is subject to review by the agency head.[147] Also, there is no right to an external review by a court.[148] Ultimately, such a directive does not have the force of law and requires the agencies to adopt it. Future Presidents can change the policy.

2. ESPIONAGE ACT

The Espionage Act[149] bars the disclosure of information regarding national defense. Sections 793(a)-(b) deal with disclosures to foreign governments, which can be punished with life in prison or death.[150] Most of the recent national security leaks have been prosecuted pursuant to Section 793(d). This section bars the willful transmission of any

---

[142] The whistleblower can inform Congressional Intelligence Committees under certain conditions. *Id.*

[143] *Id.*

[144] *See, e.g.*, Gargiulo v. Dep't of Homeland Sec., 727 F.3d 1181, 1185 (Fed. Cir. 2013); Robinson v. Dep't of Homeland Sec., 498 F.3d 1361, 1364 (Fed. Cir. 2007).

[145] Presidential Policy Directive-19, Protecting Whistleblowers with Access to Classified Information (Oct. 10, 2012), *available at* https://www.fas.org/irp/offdocs/ppd/ppd-19.pdf.

[146] Contractors are not included in the directive. *Id.*

[147] *Id.*

[148] *Id.*

[149] 18 U.S.C. §§ 793-794 (2006).

[150] *Id.*

national security document to persons "not entitled to receive it."[151] This section of the Espionage Act does not require actual harms, nor does it require that the information had been leaked to an enemy. Additionally, the leaker's belief in the value the information has to the public is also irrelevant. Each violation of this section can be punished with up to ten years in prison.[152]

IV. A POLICY PROPOSAL TO PROTECT THE FREE FLOW OF INFORMATION: PROVIDING JUDICIAL REVIEW FOR WHISTLEBLOWERS IN NATIONAL SECURITY POSITIONS

In order to promote whistleblowing, there must be a confidential channel and strong statutory protections for potential whistleblowers.[153] Without such channels and protections, potential whistleblowers will turn to the traditional press, or more disconcerting, open leak platforms.[154] The result will be unadulterated document dumping on transparency sites as we saw with Bradley Manning and WikiLeaks. Thus, Congress should amend the Intelligence Community Whistleblower Protection Act to promote internal communication.

The amendments should create an external independent tribunal to review the classification of documents, specifically when a government employee or

---

[151] *Id*.

[152] *Id.*

[153] Exec. Order 13,526 calls for federal employees to report misgiving about document classification and the ISCAP is available to review the complaints without fear of retribution to the employee. *See* Exec. Order No. 13,526, *supra* note 118. But, the ISCAP is made up of senior officials of national security agencies. This does not promote check and balances in government, nor would it be comforting to the employee. *See, e.g.*, Geoffrey Stone, *Our Untransparent President,* N.Y. TIMES, June 24, 2011, http://www.nytimes.com/2011/06/27/opinion/27stone.html?hp (arguing that the Obama Administration has not backed whistleblower protection, has prosecuted more employees for leaks, and commonly claimed states secrets privilege).

[154] *See supra* Part II.

contractor is considering leaking a document.[155] Potential whistleblowers can file a complaint with the independent tribunal and seek review of the classification.[156] Similar to traditional FOIA cases, the tribunal would conduct in-camera reviews of the national security 'secrets' to determine if the document was properly classified.[157] Furthermore, the complaint, the complainant and the judicial review will all be confidential.[158] This will protect the whistleblower and promote legal channels.[159] It will also protect the government and the confidentiality of documents that are found to be properly classified.

1. THE NEW LEGAL STANDARD FOR DECLASSIFYING NATIONAL SECURITY INFORMATION

In reviewing the classified documents, the independent tribunal should apply the following five-part test. In order to be properly classified, the government must show that the documents:

1) contain information pertinent to national security;[160] *and*
2) do not contain information about illegal government actions.[161]

---

[155] For another description of an independent tribunal reviewing government document classification, *see* Doug Meier, *Changing with the Times: How the Government Must Adapt to Prevent the Publication of its Secrets*, 28 REV. LITIG. 203 (2008). Editor's Note: Mr. Meier takes a viewpoint much different than this author. Mr. Meier argues for enhancing the government's ability to withhold information and prosecute all leakers.

[156] *Id.*

[157] For example, in the FOIA request for the torture pictures from Abu Ghraib, the court conducted an in camera review of the redacted reports and photos and decided that the interest in open government outweighs the privacy claims. *See* Am. Civil Liberties Union v. Dep't of Def., 389 F. Supp. 2d 547, 551 (S.D.N.Y. 2005). It cannot be classified only to cover-up embarrassing information. *Id.*

[158] *See infra* Part IV.A.2.

[159] *Cf.* Presidential Policy Directive 19, *supra* note 145.

[160] *See supra* Part III.C.2.

[161] *Id.*

Any documents that do not survive that test will automatically be declassified.[162] If the classification survives the first two prongs, then the government can show by *clear and convincing evidence* that the information is either:
1) not in the public interest;[163] *or* 2) it will cause "direct, immediate and irreparable harm."[164] Then the information will remained classified. Finally, the court must apply a balancing test to determine whether the benefits of declassification outweigh the benefits to the public interest.[165]

In order to promote 'whistleblowers' to use this independent review system, confidentiality will be offered to the employees who file a complaint. The proceedings will not be open to the public and the employees who filed for the review will not have their names revealed to the agency who he or she works for.[166] Furthermore, as in other whistleblower laws, employees would be immune from civil or criminal liability[167] and professional retaliation,[168] if they follow the order of the panel. Any such retaliation should be a cause of

---

[162] Similar to FOIA. *See supra* Part III.C.1.
[163] This will be similar to FOIA exemptions for privacy information and agency procedures. 5 U.S.C. § 552(b)(6). ("This section does not apply to matters that are personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."). *See also* S. Rep. No. 89-813, at 3 (1965) ("At the same time that a broad philosophy of 'freedom of information' is enacted into law, it is necessary to protect certain equally important rights of privacy . . . such as medical and personnel files.").
[164] *See* Am. Civil Liberties Union v. Dep't of Def., 389 F. Supp. 2d 547, 551 (S.D.N.Y. 2005); New York Times Co. v. United States, 403 U.S. 713 (1971).
[165] "[T]he public interest in compelling disclosure of the information . . . outweighs the public interest in gathering or disseminating news or information." *See* the Free Flow of Information Act of 2009, S. 448, 111th Cong. (currently stalled in committee).
[166] *Cf.* Intelligence Community Whistleblower Act of 1998, *supra* note 140.
[167] Congress will have to amend the Espionage Act to allow for employees to bring such documents to the independent review board. *See* Meier, *supra* note 155, at 223.
[168] Congress would have to pass a law such as the Whistleblower Protection Enhancement Act to establish such protection. *See supra* Part III.C.1.

action for a civil suit against the agency that employs the complainant.

Ultimately, the review board will serve as an ombudsman independent of the executive agencies. The composition of the independent tribunal is flexible. It could be a new independent tribunal made up of administrative law judges from different agencies[169] or Congress could instead create a new court that deals specifically with matters of government-employees relations.[170] Another suggestion is that the Foreign Intelligence Surveillance Court conduct the reviews.[171] This court consists of eleven federal district court judges from seven of the United States judicial circuits.[172] The Chief Justice of the U.S. Supreme Court appoints each judge for one seven year term, with a new judge appointed each year.[173] This court is a natural fit because of its familiarity with matters of national security.[174]

---

[169] The ALJ's could be from the agencies most likely to be the source of leaks such as the Department of Defense, Department of State, and Department of Homeland Security.

[170] Congress has the authority to create new inferior courts. U.S. CONST. art. III.

[171] *See* Meier, *supra* note 155 at 223.

[172] *Id.*

[173] *Id.* Mr. Meier contends:

> The only real change that would need to be made to the current FISA court would be to add a requirement that when reviewing the status of national security documents, more than one judge would be required to make a decision, and a majority vote would be necessary to either affirm or reject the designation.

Meier, *supra* note 155, at 222.

[174] *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 103(a)(1), 92 Stat. 1783 (1978) (codified at 50 U.S.C. §§ 1801–1871) (2012). Of course government transparency advocates would argue against the use of FISC as it rarely blocks the NSA's actions. *See* Erika Eichelberger, *FISA Court Has Rejected .03 Percent of all Government Surveillance Requests*, MOTHER JONES, June 10, 2013, http://www.motherjones.com/mojo/2013/06/fisa-court-nsa-spying-opinion-reject-request.

2. DETERRING WHISTLEBLOWERS FROM TURNING TO EXTERNAL OUTLETS

If the independent tribunal finds that the information does not warrant secret classification, then the executive agency must reclassify the documents.[175] Furthermore, the whistleblower is then free to 'blow the whistle' and release the documents to any information platform,[176] immune from civil or criminal proceedings and professional retaliation. But, when the complainants are unsuccessful in their challenge to the documents' classification, they will have two disparate choices.

First, the federal employee (or contractor) can accept the tribunal's order and return to work with the knowledge that he or she is statutorily protected, even if his or her anonymity is destroyed and he or she is retaliated against.

The second choice is to become a traditional "leaker" of classified information. But, in these cases, the "whistleblower" is now legally a "leaker" and he or she will not have any protection. The employee will be at the mercy of current laws against "leakers," including the Espionage Act.[177] Nevertheless, the original independent tribunal review will remain closed. To allow the government access to the original review would only deter people from using it.[178] More

---

[175] Then the press could access it through FOIA request, though it will not have to be automatically handed over to the press. But any FOIA request should be granted, since tribunal review will incorporate much of the consideration given in FOIA cases. However, there may be unforeseen roadblocks that Congress will have to fix by amending FOIA.

[176] This includes both traditional news media and new media platforms such as WikiLeaks.

[177] Espionage Act, 18 U.S.C. §§ 793-794.

[178] As Mr. Meier argues:

> On the other hand, if a person unsuccessfully challenges the designation and the document later ends up being leaked, the government should, at the very least, be able to use that person's identity in investigating the source of the leak. Of course, it cannot simply assume that the person was the leaker; to the contrary, it seems that the person who went to the trouble to get the document reviewed by

importantly, in cases where the information was leaked by someone other than the original complainant, it would unnecessarily punish good faith complainants who unsuccessfully used the internal check but still chose not to leak.[179]

V. CONCLUSION

During the Obama Administration, eight people (government employees or contractors) have been prosecuted for violating the Espionage Act. Prior to 2009, only three people had ever been prosecuted. In many of the recent cases, information was reported to the public through the press. It was information that served the public interest and exposed government activity that ranged from mismanagement to outright criminal. In many of these cases, the whistleblower first attempted to use legal channels and report to superiors and then to Congress, but to no avail. It was the inaction inside the government that compelled these whistleblowers to go to the press. The cost to the whistleblower was often prosecution, conviction and jail time.[180]

> the court should be presumed not to be the leaker. However, the government could talk to that person in an effort to determine the source of the leak. It is doubtful that this would have any chilling effect because, as already discussed, the people who would be inclined to use the independent review court would generally be acting in good faith and would therefore be likely to abide by the court's ruling.

Meier, *supra* note 155, at 223-224.

[179] If there was not confidentiality in the review process, the complainant would immediately become a suspect and his or her name would justifiably be associated with the leak without much recourse against the publicity. Though their job would be statutorily protected from retaliation for the original review, there are other concerns. Much of the deterrence for potential whistleblowers is the social retaliation from coworkers. *See, e.g.*, Mindy Bergman et al., *The (Un)reasonableness of Reporting: Antecedents and Consequences of Reporting Sexual Harassment*, 87 J. APPLIED PSYCHOL. 230 (2002).

[180] Edward Snowden had to leave the country and take asylum in Russia. *See supra* Part II.B.

Ultimately the system is not working. Something needs to change. This article forwards a new policy that allows for concerned employees in the national security arena to report mismanagement in good faith, with the assurance that an independent body will hear them and protect them from retaliation. At the same time, the policy allows the government to protect secrets that are truly dangerous to our national security or information which will not serve the public interest if published. The new policy does not protect leakers who do not go through the proper channels. But, under the current laws, if a good faith whistleblower wants the public to know about transgressions in the intelligence and defense agencies, then going outside of the government is the only choice and it will continue to be.[181]

[181] Current whistleblower protections "would give pause to even the most altruistic and well-intentioned whistleblowers." Stephen I. Vladeck, *The Espionage Act and National Security Whistleblowing After Garcetti*, 57 AM. U. L. REV. 1531, 1535 (2008).

LINCOLN MEMORIAL UNIVERSITY
LAW REVIEW

VOLUME 3 FALL 2015

COWARDLY TRAITOR OR HEROIC WHISTLEBLOWER?:
THE IMPACT OF EDWARD SNOWDEN'S DISCLOSURES ON CANADA AND THE UNITED KINGDOM'S SECURITY ESTABLISHMENTS

Daniel Alati[1]

The 'world's most wanted man,' Edward Snowden, might be one of the most polarizing figures in modern history. This is particularly true in the United States, where the debates pertaining to his leaks of classified information could not be more divided. Many Americans, including senior level government officials, have publicly argued that Snowden is a cowardly traitor, and have forcefully stated their belief that Snowden should return home to face a myriad of criminal charges, including those under the 1917 Espionage Act. However, many others have gone to great lengths and taken immense personal risks to support Snowden and help further his goal of bringing to light some of the most egregious surveillance abuses ever released into the public sphere.

[1] Dr. Daniel Alati is a post-doctoral researcher at the City University of Hong Kong. His doctoral studies at the University of Oxford focused on comparative anti-terrorism mechanisms in Canada and the United Kingdom.

Snowden's closest confidants are still eager to tell his story: Laura Poitras' documentary 'Citizenfour' has received rave reviews[2] and long-time NSA critic and journalist James Bamford recently interviewed Snowden in Moscow for WIRED magazine.[3] They continue to release leaked documents that expose the greatest abuses of the global surveillance machine Glenn Greenwald's website, *The Intercept,* reported recently that Canada's leading surveillance agency is analyzing records of up to fifteen million downloads daily to track extremists.[4] As a result, it seems likely that the Snowden leaks, already considered by many to be the most infamous example of whistleblowing of all time, will be a topic of American and global conversation for years to come.

However, what is less clear is what kind of tangible legislative change (if any) the Snowden leaks will bring about, particularly in countries other than the U.S. While much has been written about how the Snowden leaks have, and will continue to, influence American domestic policy and American diplomatic and intelligence-sharing arrangements with other nations, less has been written about the impact that the leaks have had on some of the U.S.' most important allies. This paper analyzes what impact the Snowden leaks have had in Canada and the United Kingdom. Sections one and two analyze the impact the Snowden disclosures have had on civil society. In doing so, it notes a glaring lack of parliamentary mechanisms for oversight of intelligence activities in Canada and also illuminates issues with the existing mechanisms in the UK. Section three examines what, if any, tangible legislative outcomes have resulted from the Snowden leaks. It concludes that it is difficult to assign any tangible legislative

---

[2] Peter Bradshaw, *Citizenfour Review – Gripping Snowden Documentary Offers Portrait of Power, Paranoia, and One Remarkable Man*, THE GUARDIAN, Oct. 16, 2014, http://www.theguardian.com/film/2014/oct/16/citizen-four-review-edward-snowden-documentary.

[3] James Bamford, *Edward Snowden: The Untold Story,* WIRED MAG., Aug. 22, 2014, http://www.wired.com/2014/08/edward-snowden/.

[4] Ryan Gallagher & Glenn Greenwald, *Canada Casts Global Surveillance Dragnet Over File Downloads*, THE INTERCEPT, Jan. 28, 2015, https://firstlook.org/theintercept/2015/01/28/canada-cse-levitation-mass-surveillance/.

outcomes in either country to the leaks. Finally, in the concluding section, recommendations for changes to the oversight mechanisms in both countries that may help to prevent the reoccurrence of some of the most egregious abuses exposed by the Snowden leaks are posited.

I. CANADA – IMPACT OF SNOWDEN DISCLOSURES ON CIVIL SOCIETY

Unsurprisingly, in the aftermath of the Snowden disclosures there was a significant amount of material published by Canadian academics, legal associations, judges, standing committee members, Parliamentarians and the media. This was to be expected as "Snowden's revelations have implicated Canada's foreign intelligence signals agency – *the Communications Security Establishment Canada* (CSEC) – in expansive domestic and foreign surveillance initiatives."[5] Some of these expansive and troubling initiatives, which implicated both CSEC and other Canadian officials, include: CSEC using airport Wi-Fi to track Canadian travelers;[6] CSEC setting up hidden spying posts in about twenty countries in which it conducted espionage at the behest of the NSA;[7] Canada allowing the NSA to spy on Canadian soil during the 2010 G8 and G20 Summits;[8] Canadian embassies overseas

---

[5] Simon Davies, *A Crisis of Accountability: A Global Analysis of the Impact of the Snowden Revelations*, THE PRIVACY SURGEON 22 (2014), https://citizenlab.org/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf.

[6] Greg Weston, Glenn Greenwald & Ryan Gallagher, *CSEC Used Airport Wi-Fi to Track Canadian Travellers: Edward Snowden documents*, CBC NEWS, Jan. 30, 2014, http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881.

[7] Greg Weston, Glenn Greenwald & Ryan Gallagher, *Snowden Document Shows Canada Set Up Posts for NSA*, CBC NEWS, Dec. 9, 2013, http://www.cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886.

[8] Greg Weston, Glenn Greenwald & Ryan Gallagher, *New Snowden Docs Show U.S. Spied During G20 in Toronto*, CBC NEWS, Nov. 27, 2013, http://www.cbc.ca/news/politics/new-snowden-docs-show-u-s-spied-during-g20-in-toronto-1.2442448.

using eavesdropping technology;[9] and, finally, allegations that Canadian spies collected metadata of phone calls and e-mails to and from Brazil's Mines and Energy Ministry.[10] While these are only some examples of deeply worrisome Canadian complicity in NSA activity, they underscore one of the most significant areas of concern to be expressed by Canadian civil society: the deep inter-connection between Canada and the United States and the corresponding connection between their intelligence activities. That Canada and the U.S. share deep economic, geographic, and cultural ties is no secret, but the extreme inter-connectedness of these two countries (and its impact on their intelligence-sharing relationships) begs further elucidation.

Farson and Teeple note that, "[t]he significance of the long-standing economic relationship with the U.S. may be even greater today for both parties, particularly given that other traditional political and military allies are now economic competitors. Certainly, it has become ever more integrated with both countries remaining each other's most significant trading partner."[11] Moreover, Farson and Teeple point to many other shared linkages between the countries that are crucial to their intelligence sharing relationships, namely, critical telecommunications and security infrastructure, and argue that Canada has been seen as a "freeloader" because of the imbalance between the two countries' differing contributions to North American defence and security.[12] Canada, like the UK, is a member of the "Five Eyes" community that

---

[9] Colin Freeze, *Canadian Embassies Eavesdrop, Leak Says*, THE GLOBE & MAIL, Oct. 29, 2013, http://www.theglobeandmail.com/news/world/canada-involved-in-us-spying-efforts-abroad-leaked-document-says/article15133508/.

[10] *Canadian Spies Targeted Brazil's Mines Ministry: Report*, CBC NEWS (Oct. 7, 2013), http://www.cbc.ca/news/canadian-spies-targeted-brazil-s-mines-ministry-report-1.1927975.

[11] Stuart Farson & Nancy Teeple, *Increasing Canada's Foreign Intelligence Capability: Is it a Dead Issue?*, INTELLIGENCE & NAT'L SECURITY, Vol. 30, 47, 59 (2015).

[12] *Id.* at 60.

> pools their resources, divide targets according to geographic location and expertise, and share analyses. In all cases, the NSA is the big brother. In some instances, it helps fund the activities of its partners in order to influence intelligence gathering programs. . . . Canada's contribution focuses on the northern regions of Russia and China, Latin America, as well the northern parts of the Atlantic and Pacific Oceans.[13]

Academic commentators have criticized various aspects of the intelligence sharing relationships between the two counties. Clement has noted that,

> [w]ell before the Snowden revelations, CIRA commissioned an expert study of the Canadian Internet infrastructure, which compared all Canadian routings with those that transited the United States and found significant inefficiencies with the boomerang routing. CIRA's report concluded that Canadian Internet access is heavily and unnecessarily dependent upon foreign infrastructure, especially US infrastructure.[14]

He laments the fact that much of Canada's internal Internet traffic is routed through the US, noting that the lack of international submarine fiber optic cables in Canada means that "almost all of Canada's third country Internet traffic is similarly routed through the United States and via NSA surveillance operations."[15] While some Canadian Internet companies, such as Bell Canada, have seized upon this opportunity to offer "safer, more private, domestic" Internet

---

[13] *Id.* at 63.

[14] Andrew Clement, *Canada's Bad Dream*, WORLD POL'Y J., Vol. 31, 25-33, 30 (2014), *available at* http://www.worldpolicy.org/journal/fall2014/canada's-bad-dream.

[15] *Id.* at 27.

solutions,[16] the post-Snowden climate in Canada still represents what Wesley Wark calls a "hopeful and distressing reality."[17] According to Wark, it is

> [h]opeful in the sense that we can anticipate a kind of recalibration of US-led global surveillance which might accord with our own principles and interests; distressing in that it reveals that Canada, enmeshed in its dependency on the NSA, and suffering problems of endemic secrecy, inadequate laws, poor accountability, hands-off political leadership, and an ill-informed public, cannot make independent headway in coming up with our own, applied Snowden verdict on global surveillance.[18]

Other than the issues noted above, there are several obstacles to the effective development and operation of a specifically Canadian system of intelligence oversight and accountability. The first is cultural. As Jeffrey Roy notes,

> [t]here is often a tendency in Canada to view such activity with a certain detachment and smugness: thank goodness that's not us. Yet, almost every significant scandal involving government action in the US has been accompanied by revelations in Canada that public sector authorities are acting in a remarkably similar manner.[19]

The second, more significant obstacle, is the lack of any established parliamentary review mechanisms that provide for

---

[16] *Id.* at 27-28.

[17] Loch K. Johnson et. al, *An INS Special Forum: Implications of the Snowden Leaks*, INTELLIGENCE & NAT'L SECURITY, Vol. 29, 793-810 (2014).

[18] *Id.*

[19] Jeffrey Roy, *Secrecy, Security and Digital Literacy in an Era of Meta-Data: Why the Canadian Westminster Model Falls Short*, INTELLIGENCE & NAT'L SECURITY, 2-3 (2015).

any kind of meaningful oversight or accountability. As will be discussed further below, attempts to set up a National Security Committee of Parliamentarians have been stymied for over a decade, despite support for such a Committee stemming from judicial inquiries, reports of parliamentary committees, civil society organizations and the wider legal community. The result is the "absence of such oversight altogether, which is how one can reasonable characterize the Canadian model. With the partial exception of Ministers directing them, Canadian Parliamentarians are shielded from scrutinizing security authorities in any direct and meaningful manner."[20]

In order to more fully understand Canada's current lack of meaningful mechanisms for parliamentary review and accountability of intelligence service activities, several stymied attempts on behalf of Canadian civil society actors over the course of the last decade must be noted. The first unsuccessful attempt to create a novel Parliamentary Committee on National Security (composed of both MPs and Senators from across party lines) occurred in 2005 under a Liberal minority government with the tabling of Bill C-81.[21] Despite cross-party support, that bill died on the order paper following the 2005 dissolution of the Canadian Parliament. The continuing lack of effective parliamentary oversight was subsequently criticized by two separate, independent judicial reviews carried out by Justices O'Connor and Iacobucci pertaining to the actions of Canadian officials in the war on terror (in particular, CSIS and the RCMP).[22] In particular, O'Connor noted that the rendition experienced by Maher Arar urgently emphasized that Canada was in need of an independent national security review framework. A Standing Committee on Public Safety and National Security tasked with reviewing Iacobucci and O'Connor's findings and recommendations would later in 2009 find it "regrettable that the government

---

[20] *Id.* at 7.

[21] Full text, legislative history, and additional information pertaining to the bill *available at* http://openparliament.ca/bills/38-1/C-81/.

[22] Government of Canada Publications, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin*, http://publications.gc.ca/collections/collection_2010/bcp-pco/CP32-90-1-2010-eng.pdf.

has not yet established the independent national security review framework recommended by Justice O'Connor" and argue that said framework was "essential to prevent further human rights violations."[23] They forcefully added that "there was an urgent need for action" and that without an integrated structure for the full review of national security issues, Canadians would be at further risk of violations of their rights and freedoms.[24]

To this date, no mechanism for parliamentary oversight of intelligence or security mechanisms in Canada, along the lines of that proposed in Bill C-81 or envisioned by Justice O'Connor, exists.[25] The ignorance of this alarming lack of oversight seems to be a trend continuing through successive Canadian governments that now continues under the current Conservative government's administration. For example, as noted by Roy,

> [a] report published by the federal Privacy Commissioner in early 2014, in line with much of the earlier analysis of the Canadian apparatus, calls for fundamental political reforms too ineffective or simply absent mechanisms for overseeing the data gathering activities of Canadian federal authorities as well as the public and private sectors more widely.

---

[23] Ottawa Standing Committee on Public Safety and National Security, *Review of the Findings and Recommendations Arising from the Iacobucci and O'Connor Inquiries*, http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=4004074.

[24] *Id.* at 11-17. Recommendation five of this report states that, "[t]he Committee recommends, once again, that Bill C-81, introduced in the 38th Parliament, An Act to Establish the National Security Committee of Parliamentarians, or a variation of it, be introduced in Parliament at the earliest opportunity."

[25] Two Bills (S-220, *infra* note 32, and C-551, *infra* note 33) have been introduced in both the House and the Senate that continue the work of Bill C-81, although neither bill has made any kind of significant progress. For example, Bill C-551 was introduced into the House in November of 2013 and has yet to progress, while Bill S-220 was introduced into the Senate in May 2014 and has still yet to pass Second Reading. *Id.*

> The report was widely applauded by Canadian security experts, though largely ignored by the Government itself.[26]

It is within this context of ignorance that the concerns of Canadian civil society echo even louder. The *Protect Our Privacy Coalition*, which is made up of more than fifty civil society organisations, has launched an online initiative calling on Members of Parliament to introduce restrictions that would curtail CSEC's most egregious abuses.[27] Moreover, the British Columbia Civil Liberties Association is constitutionally challenging aspects of CSEC's legal and operational framework,[28] and the Canadian Civil Liberties Association has also launched a lawsuit challenging the constitutionality of PIPEDA, Canada's federal data protection statute.[29] Moreover, the Privacy Commissioner has released a statement regarding telecommunications companies' responses to information requests from government authorities, in which a number of recommendations are made, particularly in regards to the transparency of authorized disclosures.[30]

In addition to these civil society actors, a number of interested Members of Canadian Parliament have tried to push for additional debate pertaining to CSEC's activities and Canada's glaring lack of parliamentary overview of

---

[26] Roy, *supra* note 19 at 17-18.

[27] *See* OPEN MEDIA, https://openmedia.ca/ourprivacy (last visited Oct. 23, 2015).

[28] The litigation is ongoing. *See* Globe Editorial, *Hey CSEC, Stop Spying on Me*, THE GLOBE & MAIL, Apr. 2, 2014, http://www.theglobeandmail.com/globe-debate/editorials/dont-spy-on-me-csec/article17781948.

[29] The litigation is ongoing. *See* Alex Boutilier, *Canadian Civil Liberties Group Launches Court Challenge on Warrantless Access*, THE TORONTO STAR, May 21, 2014, http://www.thestar.com/news/canada/2014/05/21/canadian_civil_liberties_group_launches_court_challenge_on_warrantless_access.html.

[30] *See* Office of the Privacy Commissioner of Canada, *Statement from the Interim Privacy Commissioner of Canada Regarding Telecommunications Companies' Responses to Information Requests from Government Authorities*, https://www.priv.gc.ca/media/nr-c/2014/s-d_140430_e.asp.

intelligence activities. In calling for an emergency debate on CSEC's meta-data collection program, MP Charmaine Borg argued that,

> [a]n emergency debate is needed so that parliamentarians can take an in-depth look at the extent to which Canadians' personal information, metadata and other information are collected by the police, law enforcement agencies and national security agencies. This debate is also needed so that we can look at measures that will lead to appropriate parliamentary oversight and ways to balance public and national security interests with Canadians' privacy rights.[31]

Moreover, as aforementioned, interested members of Parliament have introduced two bills (S-220[32] and C-551[33]) in order to further the work of C-81 and create a Parliamentary Committee for the oversight of national security and intelligence activities. The current Canadian government's response (or lack thereof) to the various efforts of academics and other civil society actors outlined in this section will be considered in this paper's subsequent analysis of tangible legislative outcomes to result from the Snowden disclosures.

II. UNITED KINGDOM – IMPACT OF SNOWDEN DISCLOSURES ON CIVIL SOCIETY

---

[31] *Charmaine Borg on Request for Emergency Debate*, June 13, 2013, http://openparliament.ca/debates/2013/6/13/charmaine-borg-1/only/.

[32] An Act to Establish the Intelligence and Security Committee of Parliament, http://www.parl.gc.ca/legisinfo/BillDetails.aspx?billId=6556209&Language=E&Mode=1

[33] National Security Committee of Parliamentarians Act, http://www.parl.gc.ca/legisinfo/BillDetails.aspx?billId=6256801&Language=E&Mode=1.

Whereas the Snowden disclosures in Canada and the United States sparked widespread civil society debate and condemnation, reaction to the disclosures in the United Kingdom has been markedly different, particularly in regards to the responses from the political classes. As Martin Moore notes,

> [t]he reaction in the UK has to date been startlingly different. The political class jointly defended the actions of the security services, and most shied away from proposing reform of the law. The press was split on their response, some recommending prosecution of the messenger, *The Guardian*. . . . It is difficult to explain why the reaction in the two countries has been so different. No doubt partly it is cultural, and partly due to contrasting public attitudes in the UK and US to the role of the state. It must also be due in part to the UK's intelligence services' importance to its international status. Intelligence remains one area where the UK is considered, in terms of expertise and performance, to be on a par with global superpowers.[34]

As was the case with CSEC in Canada, the material disclosed by Snowden implicated the UK's counterpart GCHQ (Government Communications Head Quarters) in various spying activities. Mark Young notes that, "British government concerns about the potential publication of classified data were significant enough to threaten *The Guardian* with legal action if the information was not destroyed. The threats prompted the destruction of hard drives containing information related to GCHQ."[35]

---

[34] Martin Moore, *RIP RIPA? Snowden, Surveillance, and the Inadequacies of our Existing Legal Framework*, THE POL. Q., Vol. 85, No. 2, 125-132, 125-126 (2014).

[35] Mark Young, *National Insecurity: The Impacts of Illegal Disclosures of Classified Information*, I/S: A J. OF LAW & POL'Y FOR THE INFO. SOC'Y, Vol. 10, 367, 368 (2014).

The United Kingdom has been placed in a particularly precarious position by the Snowden disclosures because of its relationship with the European Union. As was the case with Canada and the United States, the United Kingdom and the European Union share a vast inter-connectedness in several fields, including intelligence sharing and gathering. For instance, Bauman notes that, "[t]he UK has been in an especially delicate position given that GCHQ has participated in aggressive behavior against other partners and EU institutions while being part of the European Union and having signed the EU treaty which requires member states' loyalty."[36] Again, similar to what was the case in Canada and the United States, much of Europe's Internet traffic is routed through the United Kingdom. As Brown and Korff note, the UK

> is the landing point for the majority of transatlantic fibre-optic cables. GCHQ has reportedly placed data interceptors on fibre-optic cables conveying internet data in and out of the UK, and are able to store a significant fraction of global Internet traffic for three days on a rolling basis while carrying out further automated analysis.[37]

Despite Canada's connections to the United States, and the UK's connection to Europe, it is clear that the NSA and the GCHQ have invested more resources in their activities than any other organisations on earth. As Bauman notes,

> [t]he NSA has a budget of US $10.8 bn (7.8 bn Euros) a year, whereas within Europe GCHQ's budget of 1.2 bn Euros is well below the NSA, but nevertheless over twice the yearly budget of other agencies such as BND, FRA, or DGSE. This is why it may be more accurate to speak of

---

[36] Zygmunet Bauman et. al, *After Snowden: Rethinking the Impact of Surveillance*, INT'L POL. SOC., Vol. 8, 121-144, 127 (2014).
[37] Ian Brown & Douwe Korff, *Foreign Surveillance: Law and Practice in a Global Digital Environment*, EUROPEAN HUM. RTS L. REV., Vol. 3, 243-251, 243 (2014).

> an Anglo-American guild of professionals extended to other Western intelligence services than to analyze the network as a US-European collaboration on an equal footing, or even a transatlantic collaboration correlated with NATO.[38]

Unlike Canada, the United Kingdom does have various mechanisms for oversight of national security and intelligence activities, which has led to a variety of pre and post-Snowden analyses and recommendations for change. As Sudha Setty notes,

> [n]umerous parliamentary committees have undertaken investigations of the surveillance apparatus in the United Kingdom. A broad investigation by the Constitution Committee led to findings in 2009 that the intelligence-gathering services were largely compliant with the law, but that report included numerous recommendations for changes to surveillance authority and transparency, including giving greater consideration to civil liberties before implementing further surveillance programs, granting greater authority to various commissioners to exercise increased oversight, revisiting existing legislation to increase specificity in the surveillance authority, and making the work of the Investigatory Powers Tribunal more transparent.[39]

Writing in Martin Moore's piece, Jenna Stratford, QC agrees that there are flaws with the Investigatory Powers Tribunal, namely that "[w]here complaints are rejected, as the huge majority unsurprisingly are, claimants are not given proper reasons but instead the judicial equivalent of a 'neither confirm nor deny' notice. In addition, at present there is no possibility of appeal from the Tribunal's decisions, so that

---

[38] Bauman, *supra* note 36.

[39] Sudha Setty, *Surveillance, Secrecy, and the Search for Meaningful Accountability*, 51 STAN. J. INT'L L. 69 (2015).

probably the only recourse is to Strasbourg."[40] Furthermore, the Intelligence and Security Committee considered whether GCHQ's receipt of information by the NSA from the PRISM program was legal, ultimately finding that the GCHQ's actions were compliant with the statutory framework, but concluding that the framework required additional specificity.[41]

A further complication arises in the United Kingdom because of the operation of the Regulation of Investigatory Powers Act (RIPA).[42] As Setty notes, under the operation of this act,

> [t]he sole recourse for challenging such actions under U.K. law is making a claim to the Investigatory Powers Tribunal and that, although the Human Rights Act 1998 incorporates the European Convention on Human Rights ("ECHR") into U.K. domestic law, if the judiciary believes that a national security measure is incompatible with the ECHR standard, it may declare incompatibility but this does not constitute a mandate that the domestic security apparatus change its policies. As such, review at the domestic level has often been sharply curtailed.[43]

RIPA has been criticized by many as an outdated piece of legislation that does not fit the current realities of our technologically advanced world. Lord Ken Macdonald QC, who was the Director of Public Prosecutions in England and Wales from 2003-2008, argues that RIPA "was not written in the age of social media and big data. It is inherently

---

[40] Moore, *supra* note 34.

[41] Intelligence and Security Committee of Parliament, *Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme,* July 17, 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225459/ISC-Statement-on-GCHQ.pdf.

[42] Regulation of Investigatory Powers Act 2000, http://www.legislation.gov.uk/ukpga/2000/23/contents.

[43] Setty, *supra* note 39.

backwardlooking" and Jenna Straford echoes this sentiment by stating that, "RIPA contains only limited restrictions on the transfer of data to third-party powers. The Secretary of State has extremely wide discretion—almost unfettered in practice—to determine whether data may be transferred."[44]

Despite the aforementioned varying responses by the media and political classes following the Snowden revelations, members of UK civil society have taken issue with the political responses of the UK Government in the post-Snowden era. In the Institute for Public Policy Research's Study *Democracy in Britain,* Lord Macdonald argues that revelations about the GCHQ's Project Tempora

> point, perhaps, to an excessive and therefore damaging devotion to secrecy that appears to trump the right, even of parliament, to have a basic say in our security arrangements. The apparent manner of its conception and the government's response to its being revealed is each troubling for the light it casts on questions of oversight and democratic accountability.[45]

For Lord Macdonald, one of the most troubling aspects of what the Snowden disclosures revealed was that the GCHQ developed these capabilities while Government arguments to enact them in legislation were being successfully defeated in Parliament. As he notes, "[w]e are witnessing the creation of a very broad surveillance scheme by the backdoor – as successive governments have failed to persuade parliament that such schemes are justified or desirable – and a simultaneous growth in capacity and ambition on the part of GCHQ in the complete absence of debate, still less legislation."[46] Lord Macdonald refers to recent government attempts to suggest that Tempora is implicitly authorized by RIPA as "deeply unconvincing," questioning how it was possible that, "[i]f Chris Huhne is to be believed, the cabinet

---

[44] Moore, *supra* note 34.
[45] Guy Lodge & Glenn Gottfried (eds.), *Democracy in Britain: Essays in Honour of James Cornford*, INST. FOR PUB. POL'Y RES. (LONDON: UNITED KINGDOM) 173 (2014).
[46] *Id.* at 174.

and national security council did know [about Tempora]. They were never told."[47]

Similarly, the House of Commons Home Affairs Committee released a seething report pertaining to the current UK mechanisms for intelligence oversight,[48] in which it criticized members of the British civil service – particularly the National Security Adviser and the head of MI5 – for refusing to give evidence.[49] While the Committee did acknowledge that the Justice and Security Act[50] made some changes to the Intelligence and Security Committee, it still concluded that,

> [w]e do not believe the current system of oversight is effective and we have concerns that the weak nature of that system has an impact upon the credibility of the agencies accountability, and to the credibility of Parliament itself. Whilst we recognize the importance of limiting the access to documents of a confidential nature . . . engagement with elected representatives is not, in itself, a danger to national security and to continue to insist so is hyperbole.[51]

It also levied several criticisms towards the Investigatory Powers Tribunal and RIPA,[52] and called it "unacceptable" that there was so much confusion around the work of the Intelligence Services Commissioner.[53] In doing so, they made a number of recommendations that will be considered further in this paper's subsequent (and concluding) section on recommendations for change.

---

[47] *Id.* at 175.

[48] HOUSE OF COMMONS HOME AFFAIRS COMMITTEE, COUNTER-TERRORISM: SEVENTEENTH REPORT OF SESSION 2013-14, 66 [hereinafter *Home Affairs Committee 17th Report*], *available at* http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/231.pdf.

[49] *Id*.

[50] Justice and Security Act 2013 c. 18, *available at* http://www.legislation.gov.uk/ukpga/2013/18/contents/enacted.

[51] Home Affairs Committee 17th Report, *supra* note 48.

[52] *Id.* at 63-4, 70-71.

[53] *Id.* at 66.

III. CANADA AND THE UNITED KINGDOM – THE IMPACT OF THE SNOWDEN DISCLOSURES ON TANGIBLE LEGISLATIVE OUTCOMES

Andrew Clement has argued that, "[h]ow Canada responds to the NSA-Snowden crisis will define its identity and shape its future for decades to come."[54] Unfortunately, if the early returns are a sign of things to come, Canada is not on its way to responding to the Snowden disclosures in any kind of comprehensive or definitive manner. Granted, in the first section of this paper, several attempts were made by members of Canadian civil society to point to a glaring lack of parliamentary oversight of intelligence activities. As noted in *A Crisis of Accountability*, a joint publication published in association with the University of Amsterdam's Institute for Information Law and the Vrije Universiteit of Brussels, "[w]hile the net result has led to a greater understanding of CSEC's activities and objectives, there has been minimal concrete movement towards reform aside from some early judicial proceedings."[55] It is still unknown at this point whether either of the aforementioned constitutional challenges launched by the British Columbia Civil Liberties Association or the Canadian Civil Liberties Association will lead to fruitful reform. Despite a very active civil society, responses from the current Conservative government have been sparse.

Hopes for future tangible legislative outcomes are further called into question by the past track record of successive Canadian governments. For over a decade now, various iterations of Bill C-81 (which would enact a National Security Committee of Parliamentarians to provide *some* form of parliamentary scrutiny of intelligence activities) have died in successive Canadian parliaments, despite cross-party support in 2005 at the time of the bill's inception. At that time, political instability associated with successive minority governments (and the corresponding dissolution of Parliament) could easily be assigned blame for the demise of Bill C-81. However, as Roy Notes, "[i]f partisan collaboration is rare and tenuous during minority regimes, it is quickly

---

[54] Clement, *supra* note 27.

[55] Davies, *supra* note 5, at 22.

forgotten once majority status is returned since the victors see little compelling reasoning in sharing unfettered power with its now-defeated opponents."[56] The aforementioned current iterations of the bills (Bills S-220 and C-551) have been moving through Parliament at a snail's pace, *despite* the impetus placed on them by the Snowden revelations. Even before the Snowden revelations, two separate judicial inquiries by Justices Iacobucci and O'Connor (both of which attracted significant public attention) called attention to an alarming lack of parliamentary oversight of intelligence activities in Canada. To date, the recommendations of these inquiries have still not been taken up by the Canadian government, despite the fact that the Standing Committee on Public Safety and National Security has reiterated their importance. While Canadians often enjoy debating the potential shortcomings of the US Congressional model, "other likeminded democracies have or are also forging more robust oversight and review mechanisms that are likely to prove increasingly consequential in balancing competing interests of security, secrecy and privacy in an environment of digital connectedness and information abundance."[57] Canada can ill-afford to stay stagnant in a world that continues to evolve and produce new digital realities. Nor can it afford to hope that its civil society or its courts will spur the Canadian government to action.

To contrast, the issue in the UK is certainly not a lack of parliamentary oversight mechanisms of intelligence activities, but rather the appropriate means through which existing legislation and mechanisms should be refined. For the most part, the UK Government has responded with silence and secrecy, even going so far as to attack *The Guardian* and force them to destroy material that would be damaging to the GCHQ. It has been noted that, "Deputy Prime Minister Nick Clegg has ordered an 'Obama-style' review of intelligence agencies, to be led by the Royal United Services Institute, but the report will not even be released until after the May 2015 elections."[58] As a result of this government response, Brown and Korff have argued that, "[i]t seems judicial intervention will be required to bring the UK's legal framework back into

---

[56] Roy, *supra* note 19 at 8.

[57] *Id.* at 22.

[58] Davies, *supra* note 5, 70.

compliance with the Human Rights Convention."[59] As noted above by Setty, even successful litigation may not bring about effective change because of the UK's complex arrangements under RIPA, the European Convention for Human Rights and the Human Rights Act. As a result, "[w]ithout a Snowden-like disclosure to enable such review, or a strong commitment by the United Kingdom to abide by the human rights standards articulated at the European level, parliamentary oversight would be the key mechanism to protect against overreaching by the British intelligence community."[60]

If parliamentary oversight is to be the key mechanism to protect against future overreaching of the British intelligence community, then the recommendations put forward by UK civil society members, in particular Lord Macdonald and the House of Commons Home Affairs Committee, need to be taken seriously. While some may argue that the 2013 Justice and Security Act attempted to do just that,[61] others are more skeptical. As Lord Macdonald notes,

> [t]he Justice and Security Act passed last year handed marginally more power to the ISC, but did little to correct executive control over it. For example, each committee member is now appointed by parliament but must first be nominated for membership by the prime minister. The ISC now has the power to call for evidence or information from ministers and agencies; however, the means and manner in which information can be provided to the ISC must be outlined through a memorandum of understanding with the prime minister. In the

---

[59] Brown & Korff, *supra* note 37 at 6.

[60] Setty, *supra* note 39 at 28.

[61] Home Affairs Committee 17th Report, *supra* note 48 at 62. "A number of witnesses to this inquiry took the opportunity to highlight the improvements to the Intelligence and Security Committee which were contained within the Justice and Security Act 2013. There were suggestions that the committee ought not to be judged on its previous failures but rather time ought to be given to see how it worked under the new regime." *Id.*

> light of the Snowden revelations, it seems that reforms in the J&S Act did not go far enough. Moreover, we also need to consider the extent to which RIPA can be said to remain an adequate mechanism for regulating surveillance activities.[62]

Even if one accepts the argument that the Justice and Security Act was an attempt to respond to deficiencies in the oversight of intelligence activities, this paper has noted the concerns of several academics and civil society actors pertaining to various other pieces of legislation and mechanisms, including RIPA and the Investigatory Powers Tribunal, that have not been consequentially amended by that Act. These still require further attention on the part of the UK Government before any true tangible legislative outcome can be assessed to the Snowden disclosures.

IV. CONCLUSION – RECOMMENDATIONS FOR FUTURE CHANGE

Despite the apparent conclusion that neither the Canadian nor the UK government has responded to the Edward Snowden disclosures with tangible, consequential legislative changes, it cannot be said that these disclosures have had no impact. The revelations provided for by the Snowden documents have fundamentally changed public perceptions in both countries about how intelligence activities are carried out and have sparked civil society commentary amongst academics, judges, legal practitioners, interest groups and the media pertaining to how oversight of intelligence communities should be improved in the future. The immense energy and analysis that has gone into these various commentaries should not be lost. As Wesley Wark argues,

> [w]hatever badge we stick to Mr. Snowden (and his media collaborators) may in itself not matter very much, and certainly will be dwarfed by the issue that he has called our

[62] Lodge & Gottfried, *supra* note 45 at 176.

> attention to. That issue is the practice, and future, of global electronic surveillance by state intelligence agencies. The ultimate verdict(s) regarding Edward Snowden the man will pale in significance alongside the verdict(s) on global surveillance.[63]

With that in mind, this paper will now conclude by reiterating some of the most important changes that urgently need to be considered by both Canada and the UK going forward into a post-Snowden future.

For Canada, the most urgently needed change required is clear: the work of Bill C-81 needs to be fast-tracked through its current iterations, either Bill S-220 or C-551, so that the country may finally have some form of parliamentary review and oversight of intelligence activities. The Canadian government should not need to be implored to do this through damaging revelations of sensitive material, which will undoubtedly continue in the future (as noted at the outset of this paper, a new *Intercept* story pertaining to CSEC's spying was released only recently). Various successive Canadian governments have for too long ignored a glaring deficiency in Canada's overall national security apparatus. Two separate judicial inquiries have been commissioned (at no small expense to the Canadian taxpayer) and both have recommended the immediate need for additional review mechanisms. These recommendations have been further bolstered by the Standing Committee on Public Safety and National Security, and have been demanded by various civil society actors noted in this paper. The Canadian government is poised to introduce a whole new set of anti-terrorism laws that it has been working on since last year's attack on Parliament Hill.[64] There is growing concern that this new package of laws will actually increase powers of various

---

[63] Loch K. Johnson et. al, *An INS Special Forum: Implications of the Snowden Leaks*, INTELLIGENCE AND NATIONAL SECURITY, Vol. 29, 793-810, 810 (2014).

[64] Jim Bronskill, *Five Things to Know About Canada's New Anti-terrorism Measures*, CTV NEWS, Jan. 30, 2015, http://www.ctvnews.ca/canada/five-things-to-know-about-canada-s-new-anti-terrorism-measures-1.2213071.

intelligence and police agencies.[65] These concerns are further exacerbated by the fact that Canada has no genuine accountability mechanisms for the oversight of these agencies, or for its national security apparatus as a whole. It is simply irresponsible for the Canadian government to go forward with new counter-terrorism legislation without addressing this glaring gap in its current national security framework.

In contrast to Canada, the United Kingdom is significantly ahead in regards to existing infrastructure for parliamentary oversight and accountability of intelligence activities. That being said, there are a number of targeted recommendations for change that could significantly improve these oversight mechanisms, were they to be acted upon by the UK government. In particular, Lord Macdonald suggests six additional reforms: 1) The ISC should become a full joint parliamentary select committee; 2) it should be appointed by and responsible to both Houses of Parliament; 3) it should have stronger powers to obtain evidence. These should include the power to obtain information, by summons, from outside parties, lay experts, ministers and civil servants, as well as from security chiefs; 4) it should have an independent secretariat and independent legal advice, and it should have access to all information. Select committee procedures already allow the exclusion of material whose publication might be harmful and the disclosure of such material is a serious criminal offence; 5) it's chair should be a member of the opposition and should not be someone who has previously held responsibility for any of the security agencies; 6) Finally, we need to increase the level of institutional expertise to ensure that human rights are put at the heart of policy and strategies in this area, at a level that is more than rhetorical. We need to consider how such a committee could develop a wider role in educating parliament as a whole and, consequently, the public.[66]

Similarly, the House of Commons Home Affairs Committee makes a number of recommendations that echo those of Lord Macdonald. They also believed that there were

---

[65] Andrea Janus, *Spy Service to Get Stronger Under Federal Bill*, CTV NEWS, Jan. 30, 2015, http://www.ctvnews.ca/canada/spy-service-to-get-stronger-under-federal-bill-1.2213119.

[66] Lodge & Gottfried, *supra* note 45 at 178-179.

several ways in which the ISC could be strengthened: 1) election of the membership of the Committee by the House of Commons; 2) the Chair of the Committee being a member of the Opposition and not a former Minister with responsibility for any of the agencies; 3) ensuring that the Committee has access to relevant expertise (for instance in terms of the technological aspect of the work carried out by the security and intelligence agencies); 4) allowing other Parliamentary Committees to scrutinize the work of the security and intelligence agencies.[67] The Committee also recommended that the Investigatory Powers Tribunal be legislatively compelled to produce an annual report on their work, containing at the very least the number of cases it has received and the outcome of cases determined in that year.[68] Finally, in regards to RIPA, the Committee argued that,

> [g]iven the criticism which the Regulation of the Investigatory Powers Act is subject to, we believe that the legislation is in need of review. We recommend that a Joint Committee of both Houses of Parliament should be appointed in order to hold an inquiry with the ability to take evidence on the Act with a view to updating it. This inquiry would aim to bring the Regulation of Investigatory Powers Act up to date with modern technology, reduce the complexity (and associated difficulty in the use of) the legislation, strengthen the statistical and transparency requirements and improve the oversight functions as are set out in the current Act.[69]

Although both Canada and the UK have very different starting points for how they should oversee their intelligence activities in the future, the motive behind both is the same. Civil society confidence in the ability of both governments to protect the privacy of their citizens reached an all-time low following the Snowden disclosures. As is noted by Bauman,

---

[67] Home Affairs Committee 17th Report, *supra* note 48 at 62.
[68] *Id.* at 63-64.
[69] *Id.* at 70-71.

> [o]nly 5% of respondents in Canada trust government to guard their data, and this only rises to 7% in the United States. Whether in the United States, Canada, or the UK, it is clear from these results that a substantial proportion of the population are concerned about government surveillance and that there is a high degree of cynicism about what governments do with those data.[70]

Members of civil society in both countries are doing what they can to compel their governments to act, but there is only so much they can do if their governments are unwilling. Both Canada and the UK need to start treating the Snowden disclosures as an opportunity to reassess how they collect intelligence, when they collect intelligence, who they share intelligence with and, perhaps most importantly, how they oversee the collection of that intelligence.

[70] Bauman, *supra* note 36 at 141.