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).